

Thomas H. Lenhard

Data Security

Technical and Organizational
Protection Measures against
Data Loss and Computer Crime

Data Security

Thomas H. Lenhard

Data Security

Technical and Organizational
Protection Measures against Data
Loss and Computer Crime

Thomas H. Lenhard
Comenius Universität
Bratislava, Slovakia

ISBN 978-3-658-35493-0 ISBN 978-3-658-35494-7 (eBook)
<https://doi.org/10.1007/978-3-658-35494-7>

This book is a translation of the original German edition „Datensicherheit“ by Lenhard, Thomas H., published by Springer Fachmedien Wiesbaden GmbH in 2020. The translation was done with the help of artificial intelligence (machine translation by the service DeepL.com). A subsequent human revision was done primarily in terms of content, so that the book will read stylistically differently from a conventional translation. Springer Nature works continuously to further the development of tools for the production of books and on the related technologies to support the authors.

© Springer Fachmedien Wiesbaden GmbH, part of Springer Nature 2021

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Fachmedien Wiesbaden GmbH part of Springer Nature.

The registered company address is: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Contents

1	Introduction	1
2	Data Protection and Data Security	3
3	How Computers Communicate with Each Other	5
4	What Can Happen to Data?	15
5	Hazards in the Technical Environment	17
6	Dangerous Software	25
6.1	The Trojan Horse	27
6.2	The Virus	31
6.3	The Logical Bomb	34
6.4	The Keylogger	35
6.5	The Sniffer	35
6.6	The Back Door	39
7	Removable Media, USB Devices, Smartphones and Other Mobile Devices	41
8	Telephone Systems	45
9	The Greatest Danger in a Digitalized World	51
10	Data Destruction	55
11	Data Backup and Restore	61
12	Encryption	65
13	Website Hacking	69

14	Common Security Problems	73
14.1	Working Consoles that Are Not Locked	73
14.2	Printer Stations and Multifunction Devices	74
14.3	Working with Administrator Privileges	74
14.4	The Internet of Things and Industrial Control Systems	75
15	Identification of Computers and IP Addresses	77
16	The Firewall	81
17	The Router	85
18	Configuration of Security Systems	87
19	The Demilitarized Zone	93
20	Organizational Data Security	99
21	Notes	101
	Closing Words	105
	Literature	107
	Index	109

Abbreviations

Cat-7	Cable Category 7
CCC	Chaos Computer Club
CRM	Customer relationship management
CTI	Computer telephony integration
DBMS	Database management system
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized zone
DNS	DNS
DVD	Digital Versatile Disc
EN 50173-1	European Normative 50173-1:2011 about Information technology—Generic cabling systems—Part 1: General requirements
ERP	Enterprise resource planning
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISO	International Organization for Standardization
LLC	Logical link control
MAC	Media access control
NAS	Network attached storage
NTFS	New technology file system
NTP	Network Time Protocol
OSI	Open System Interconnection
PBX	Private branch exchange (telephone system)
PGP	Pretty Good Privacy
POP	Post Office Protocol
RFID	Radio-frequency identification

RJ45	Registered jack 45
SFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSD	Solid-State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transaction Control Protocol
Telnet (TNP)	Telecommunication Network Protocol
TLS	Transport Layer Security
UNC	Uniform Naming Convention
USB	Universal Serial Bus
UPS	Uninterruptible power supply
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual private network
WEP	Wired Equivalent Privacy
WLAN	Wireless local area network
WPA	Wi-Fi Protected Access

List of Figures

Fig. 3.1	The OSI model	7
Fig. 3.2	Additional information in the address field of the browser	12
Fig. 3.3	Ping	13
Fig. 5.1	A server cabinet in the deepest cellar of the building	18
Fig. 5.2	A steel tray to protect IT equipment from pipes	20
Fig. 5.3	Chaos in a part of a clinical “computer centre”	22
Fig. 6.1	Wireshark analyzing database queries	36
Fig. 8.1	Separation of IT and telephone network	48
Fig. 10.1	Calibre .44 Magnum and other creative ideas are not suitable as a secure method of data destruction	58
Fig. 19.1	Positioning of a DMZ network	94

List of Table

Table 3.1 Services and port numbers 10



Introduction

1

Abstract

Data security is an inseparable part of data protection. While data protection is defined by national or international laws and is thus subject to the greatest differences worldwide, the same technology is used almost everywhere in the world, so that it can be expected that data security problems will be at least similar everywhere in the world. The introduction to this publication addresses in particular the fact that a global network also entails cross-border problems and challenges.

Data protection law varies from nation to nation and sometimes even within a nation from region (state, canton, department, etc.) to region. However, in a globalized world with almost unlimited data traffic over the Internet, activities and criminal acts do not end at any national border. Of course, there are exceptions to this: In some states, where concepts such as freedom or human rights are interpreted differently than in the rest of the world, restrictions on the Internet and free access to information must sometimes be expected. This publication addresses fundamental issues of data security. Therefore, political positions and views are not discussed here. While legal regulations in different nations or states of the world sometimes differ fundamentally, we use the same operating systems, the same types of servers, the same hardware, the same notebooks, printers and other computer equipment every day. And this is completely independent of the country in which we live or work. At the moment these lines are being written, it is possible that criminals from somewhere in the world are trying to attack the author's computer, which is currently located in Germany. The Internet makes it possible to attack millions of

computers worldwide while the attacker is sitting comfortably at home in his living room.

In the context of this publication, we understand the Internet as an unlimited, worldwide network with a high risk potential. Such a network was only feasible due to technical standards. The fact that we use globally accepted and used communication standards to transport files, messages and information over the Internet from one end of the world to the other, as well as the omnipresent threats in the context of Internet use, result in a deeper consideration of the overall situation in an axiom that should underlie the considerations of this publication:

Data Security Measures Can Be Implemented Worldwide in Identical Form

But even if technical methods can—theoretically—be used anywhere in the world, the author of this book does not want you to come into conflict with national or local law in any way. So: please keep in mind that the use of some technical methods, devices or even certain software might be prohibited or restricted by law in your country. There are currently many countries worldwide that have legal restrictions when it comes to the use of cryptography and encryption systems, for example. At this point, however, it should be pointed out that dangers to data and systems do not only lurk on the Internet.

The following chapters explain the basics of computer technology that are necessary to understand the extent and danger of cybercrime. In particular, other dangers with regard to data security are also described and solutions are presented as to how systems can be secured.



Abstract

Data protection is inconceivable without data security. But data security encompasses much more than just measures to protect personal data. The term data security is also by no means limited to the defense against hacker attacks. This chapter therefore provides an initial insight into the scope and tasks of data security.

If you search the Internet for the terms data protection and data security, you will find numerous definitions, some of which differ fundamentally from one another. A consistent and common definition of what constitutes or includes data protection inextricably links this term with the protection of personal data. For example, if you search for the term “data protection” on the European Community website, you will be directed to the chapter on “protection of personal data”.¹ This publication follows such a definition of the term “data protection”. This term is therefore used in the following as a general term for the protection of personal data. At the same time, data security can be understood as an essential component of data protection, which describes technical and organizational measures.² While the focus of data protection is only on personal data, data security does not distinguish between personal and non-personal data. As far as security devices, such as a firewall, (see Chap. 16) are installed to protect the computer network of a company or institution, such measures

¹<http://ec.europa.eu/justice/data-protection/>. Accessed 28.12.2016.

²DIRECTIVE 95/46/EC Of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

will protect all kinds of data in the company network from external attacks via the Internet.

From a technical point of view, it does not matter whether the protected data are patents, chemical formulas, economic data, construction plans or personal data.

The focus of this publication is on data security. Therefore, no distinction is made in the following chapters between data with or without personal reference. Rather, only the abstract term “data” is used in the following. With regard to the topic of data security, which is dealt with here, it must be pointed out, however, that its scope is by no means limited to the processes that take place within computers or computer networks. Rather, this discipline also deals with questions of fire protection or the defense against espionage and sabotage.



How Computers Communicate with Each Other

3

Abstract

If you want to repair a complex machine, it is first of all necessary to know how it works. It is no different with the highly complex topic of data security. Before one can correctly assess threats to the security of IT systems, it is necessary to know how these systems work and, in particular, how computers communicate with each other. This chapter therefore conveys basic knowledge in order to understand why security problems repeatedly occur in the environment of computer communication.

A computer virus can only infect a computer if that computer communicates with other local computers or with other computer systems on the Internet. Although, there is still the way to infect a computer via external data carriers, definitely no computer virus will develop on an isolated computer by itself. In order for a computer system to become infected, it is always necessary for some form of contact with the outside world to occur.

This can be done, as mentioned earlier, by transporting a malicious program on an external device that is connected to the computer. Or, to remain in the context of communication, the system can be infected via the Internet, with the virus or malicious program then being transferred to the respective system from another computer or server on the Internet.

To develop a better understanding of activities and measures related to data security as described in this book, it seems useful to first explain how computers

communicate with each other. The most commonly used protocols in the “computer world” are TCP/IP.¹

Although there are other protocols that could be used in place of TCP/IP, such as SPX/IPX, the former are considered here because their importance, as well as their prevalence, far exceeds that of alternative protocols at the respective communication levels. The Encyclopaedia Britannica explains a protocol in the context of networking as “*a set of rules or procedures for transmitting data between electronic devices, such as computers. In order for computers to exchange information, there must be a preexisting agreement as to how the information will be structured and how each side will send and receive it.*”²

Regardless of whether we use an Internet browser to visit a website or whether we want to connect to one of our company’s servers from our tablet PC or smartphone, this always requires a connection and corresponding protocols to establish the communication. The way in which this network-based communication is realized is defined in a seven-level model. The model is generally referred to as the OSI Reference Model,³ where OSI stands for “Open System Interconnection”.⁴ This model is explained below (Fig. 3.1) as a basis for understanding further descriptions in this book.

The layers of the model are numbered starting with the lowest level. Level 1 stands for the physical layer of a connection. This layer describes the physical transmission medium or the physical transmission path. This can be a copper cable or a fiber optic cable. However, it can also be a radio connection, an optical connection or a combination of several transmission media. Even though this layer is the lowest layer of the OSI model, it is here that the causes of communication problems in networks are most frequently found.

High-frequency technology is used within level 1 (physical layer) of the OSI layer model. Here, at the same time, basic protocols are defined as to how bits are sent and received according to the specifications of the medium used. Therefore, this layer can definitely be considered the most complex layer of the OSI model.

The second layer of the described model is the data link layer. The most familiar element at this level is probably the MAC⁵ address (MAC).

¹Transaction Control Protocol/Internet Protocol.

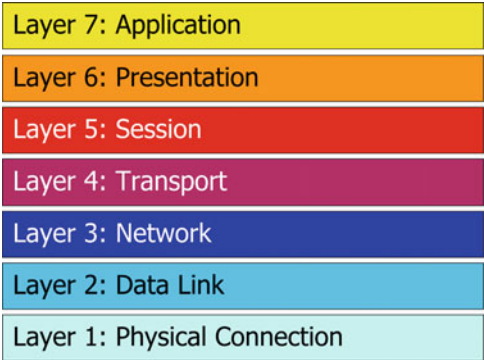
²<https://www.britannica.com/technology/protocol-computer-science>. Accessed 10.07.2021.

³C. Hunt, TCP/IP Network Administration, 3rd ed. O’ReillyMedia Inc., Sebastopol (USA), 2002.

⁴ISO/IEC 7498-1.

⁵Media Access Control.

Fig. 3.1 The OSI model



The MAC is a unique physical network identifier, which identifies the network adapter. Since this MAC address is—at least theoretically—unique worldwide, the manufacturer of a network adapter or network card can be identified in most cases because the MAC address contains a manufacturer code. MAC addresses are written in hexadecimal notation or in a mixed code that displays the manufacturer ID in plain text. As shown in the following example, the MAC address can identify the manufacturer of IT equipment. Since nowadays most large manufacturing companies operate according to ISO 9000 and are certified accordingly, it is possible to identify the type and serial number of devices by their MAC address. The following example shows two notations for one and the same MAC address (Table 3.1).

Example: Notation of MAC-Addresses

MAC (hexadecimal notation):	7F A0 00 1F 69 CF
MAC (mixed case):	<COMPANY> 1F 69 CF

As shown in this example, the hex code 7F A0 00 (chosen arbitrarily here) can identify a manufacturer. In many cases, it is also possible to trace the path from the manufacturing company to the customer/user, especially if devices are supplied to customers via direct sales. However, this is explained in detail in Chap. 15. ◀

However, there is a lot more to explain about layer 2 of the OSI model: Layer 2 can be divided into two further layers. One sublayer deals with the MAC address, which has already been addressed. The second sub-layer within the second layer is the LLC⁶ part. This logical connection control is the part of Layer 2 that communicates with Layer 3, while the MAC part communicates with the physical layer, i.e. with Layer 1.⁷

Layer 3 is called the network layer. This is a bit confusing, because all layers of the OSI model are essential components of functioning network communication. In languages other than English, this layer is therefore sometimes referred to using terms that mean switching or exchange. The job of this layer is to ensure that packets find the right path between sender and receiver. The best known protocol that operates at this layer is IP.⁸ Therefore, network address, such as the IP address, belong to this layer.

The fourth layer of the OSI model represents the transport layer. The most frequently used protocol of this layer is TCP.⁹ This protocol works with data packets in which messages or parts of messages are transported. Parts of messages are transported because a data packet has a predefined size and thus the payload of the packet is limited. Accordingly, messages or files transmitted over a network connection must be distributed over several data packets. To ensure that the receiving computer assembles a message or file in the correct order, the packets use sequence number. So, to pick an example, if a text is too long for one packet, it will be split into multiple packets. The receiver (computer) will reassemble the contents of these packets according to the sequence numbers sent along.

If the transmitted content of TCP packets is not encrypted, messages, passwords or other transmitted texts can be read relatively easily by unauthorized third parties, as far as there is a possibility to log the data packets of a communication process. Such problems are considered separately in Sect. 6.5.

The fifth layer of the OSI model is called the session layer. The main purposes of this layer are to establish a session and to ensure fault-tolerant synchronization by

⁶Logical Link Control.

⁷<http://www.netzwerke.com/OSI-Schichten-Modell.htm>. Accessed 31.03.2016.

⁸Internet Protocol.

⁹Transmission Control Protocol.

using synchronization points. Protocols such as FTP,¹⁰ SMTP,¹¹ HTTP,¹² POP¹³ or Telnet (TNP) are found on this layer.¹⁴

To avoid confusion, however, it must be mentioned here that some protocols, such as HTTP, are also found at higher levels than the fifth layer.

Level 6 and Level 7 describe the presentation and application layers of the OSI model. Level 6 uses code pages, i.e. predefined character sets, to ensure that data is presented in a readable manner.

As the name of level 7 already implies, this is the layer on which data input and data output take place.

Before we can start thinking about the various dangers and the protection of our data, however, some basic explanations are necessary: Services are applications or programs that can be run permanently on a computer as a background process. Such services can serve very different purposes and tasks.

For example, if we want to upload files from a remote server to our local system through the File Transport Protocol (FTP), it is necessary that the FTP server service is running on this remote server. Such a program is usually not displayed on a desktop while it is running. The FTP service, is a “classic” background process that is usually started immediately after the computer is switched on and the operating system is loaded.

But how does a computer system find this service in the network? The computer that wants to access or use the corresponding service on a remote server first uses the IP address (OSI layer 3) to communicate with the correct server. But how does the server, which is located somewhere on the Internet, know that our local computer wants to communicate with the FTP service? In particular, this question arises against the background that servers often run several different services (for example, HTTP, HTTPS¹⁵) simultaneously. Services that communicate over a network use so-called port or port number as an additional identifier. Such additional identifiers are standardized worldwide. Wherever we want to communicate using a standard FTP protocol, we use port number 20 for data transfer and port number 21 for commands.¹⁶ After all, this means nothing more than that to establish a remote

¹⁰File Transport Protocol.

¹¹Simple Mail Transfer Protocol.

¹²Hypertext Transfer Protocol.

¹³Post Office Protocol.

¹⁴Telecommunication Network Protocol.

¹⁵Hypertext Transfer Protocol Secure.

¹⁶Dausch, M., *Netzwerke-Grundlagen* p. 82, Herdt-Verlag, 2014.

Table 3.1 Services and port numbers

Service	Port number
FTP (Commands)	21
SSH ^a	22
TELNET	23
SMTP	25
HTTP	80
POP3	110
NTP ^b	123
HTTPS	443
WHOAMI ^c	563

^aSecure Shell
^bNetwork Time Protocol
^cWhoami (who am I) returns as command-line command the user name with which the user is currently logged in

connection to any service, the IP address and port number are necessary. The combination of both is called a **socket**. Table 3.1 shows examples of some services with their corresponding port numbers.

System ports use port numbers between 0 and 1023. From 1024 to 49,151, the ports are referred to as userports. In the range between 49,152 and 65,535, a distinction is made between dynamic and private ports.¹⁷

Since a socket is used to establish a connection with a special service, it is necessary that this addressed service also reacts to incoming requests. It “listens” quasi permanently, whether any message arrives at it. As we will see later, this circumstance can lead to massive security problems.

So far in this chapter, we have learned about sockets, which are built from port numbers and IP addresses. It was also explained that the IP address is elementary for identifying a computer and finding the right path for a data packet. Therefore, it is a logical consequence that we also have to take a closer look at the IP address before the end of the chapter.

The classic IP address is now referred to with the short form IP4. The number four is therefore added to document that the corresponding IP address uses four (4) bytes to represent the address. Such an IP address may look like the following:

192.168.2.17

¹⁷ <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>. Accessed 27.07.2021.

As already mentioned, an IP address of this type is constructed from four bytes. However, the IP4 does not use these bytes to define a single large number, but distributes the bytes over four segments, each separated by a dot. Each of these segments thus has one byte available to define its value. Since a byte consists of eight bits, it is not possible to define a number higher than 255 with the binary code of a byte. Therefore, the IP address (IP4) is constructed from four numbers, all of which are in the range from 0 to 255. This classic IP address is supplemented by a subnet mask, which also consists of four segments, each defined by one byte. The task of this subnet mask is to divide the IP address into two segments. These parts represent the network ID and the computer ID, i.e. they identify both the computer and the network to which it is logically assigned.

The following example shows how this subdivision works:

Example

IP address:	192.168.002.017 (Note: 002 = 2; 017 = 17)
Subnet mask:	255.255.255.000

In this example, the network -ID is “192.168.002” while the computer ID is 017. If we were to change the subnet mask to “255.255.000.000”, the network ID would be “192.168” while the computer ID would be “002.017”.

The system of separation between network ID and computer ID can be much more complex, however, because the subnet mask can take values other than 255 or 000. For example, they could also contain the value 192 in a segment, so that the separation between network ID and computer ID would run within this segment. However, this detail will not be relevant for further explanations. The only information we should remember in this regard is that computers in the same network segment of a local network cannot communicate if the subnet masks are different.

Now you will ask how this system of IP addresses and ports (IP address + port = socket) works when a connection to a web page somewhere on the Internet is to be established via a web browser. Let us assume that you want to visit the author’s website. Then you can paste the web address “www.it-planung.com” into your browser and the next moment some information will be added to the address bar of the browser, as it is shown in Fig. 3.2. In this example, the

Fig. 3.2 Additional information in the address field of the browser



protocol (HTTPS) has been automatically added to the address field. This protocol is represented by the port number 443 (see Table 3.1). The web address (www.it-planung.com) is translated into an IP address on special DNS¹⁸ servers on the Internet.

In this example, the address of the web page during the test was IP 217.160.231.189. The IP address of a web page is easy to find out. All you need is the command shell¹⁹ of a computer that is connected to the Internet. The command “Ping” then queries the IP address of a specified target and returns the corresponding result. Figure 3.3 shows the use of the “Ping” command in a command shell. By the way, the ping command is available on almost all common operating systems.

Now we have all the information we need to build a socket to connect to this server. But there is one more detail to consider before we try to call the page directly by specifying the socket. The page used here is hosted by an Internet provider, not on the company’s own server. The company used for the example also does not have its own permanent IP address, but obtains a dynamic IP address from the provider for Internet connections when the connection is established. This means that it is generally not possible to call up the website used via the IP port combination. However, where companies operate their own web server and also have their own website, it is possible to enter an IP port combination (socket) in the address field of the browser instead of a written-out web address (e.g. Fig. 3.2). The DNS servers on the Internet can translate names into IP addresses as well as IP addresses into names. An entry in the address line of the browser would then look something like this:

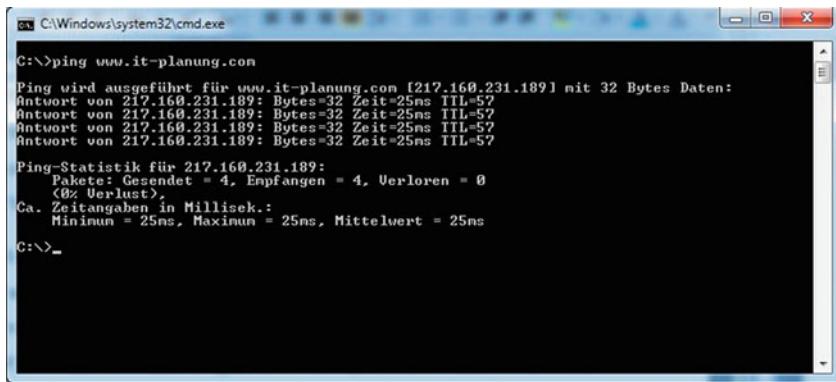
```
//<IP address>:80
```

By specifying the port, it is defined that a connection is to be made via HTTP.

Due to the explosive growth of the Internet, it has become necessary in recent years to provide more IP addresses than could be generated by means of the four

¹⁸Domain Name Service.

¹⁹Command line.



```
C:\Windows\system32\cmd.exe

C:\>ping www.it-planung.com

Ping wird ausgeführt für www.it-planung.com [217.160.231.189] mit 32 Bytes Daten:
Antwort von 217.160.231.189: Bytes=32 Zeit=25ms TTL=57
Antwort von 217.160.231.189: Bytes=32 Zeit=25ms TTL=57
Antwort von 217.160.231.189: Bytes=32 Zeit=25ms TTL=57
Antwort von 217.160.231.189: Bytes=32 Zeit=25ms TTL=57

Ping-Statistik für 217.160.231.189:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
            (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 25ms, Maximum = 25ms, Mittelwert = 25ms

C:\>_
```

Fig. 3.3 Ping

octets (segments) of the classic IP address. Therefore, the IPv6 was developed. This uses 128 bits for addressing, which corresponds to 16 bytes. However, addresses according to the IPv6 standard are no longer represented by numbers between 0 and 255, but are written in hexadecimal code, whereby the address consists of eight address blocks, each separated by colons.

The eight address blocks are written inside square brackets and a port to be addressed is added to the closing bracket preceded by a colon. An IPv6 address can look like this:

`http://[337C:4EAA:F034:4C17:4450:AF3E:1203:B7C3]:80`

Such an address should be a globally unique identifier for a computer. ◀



What Can Happen to Data?

4

Abstract

Careless administration of systems or careless storage of IT systems in basements can sometimes cause more damage than an attack by hackers. This chapter therefore provides an overview of what can happen to our data. Data loss is just as serious as unauthorized access to our data.

When we hear the term data security, many of us immediately think of the cliché of the evil hackers sitting in some dark room trying to steal our data. But hackers are just one of many threats to data security.

First, therefore, let us look at an ordinary workstation computer (PC). Without any external intervention, the power supply and the hard disk are the parts of a computer that most frequently fail due to a defect. As far as a conventional hard disk fails, the cause is either found within the electronic circuits or mechanical components have been damaged. As far as mechanical damage is concerned, it is usually much more difficult to recover data and data structures on a hard disk. In such a case, data recovery can be very expensive and sometimes, depending on the type and extent of damage, it is not even possible to recover stored data in whole or in part. In such a case, if there is no working backup available or in place, data may be irretrievably lost. It should always be kept in mind that this is not exclusively a problem of commercial enterprises, organizations or institutions. Even when using a private computer, such a data loss can have serious consequences, because on this kind of computer often not only snapshots of the last vacation are stored. Many private individuals use their computers to organize their lives. In the event of a computer failure, tax documents, important e-mail communications, address books,

insurance documents, other contract documents and other important data, information and electronic documents could be lost.

If we now think about what such a data loss could mean for a company, we come to the conclusion that the continued existence of a company could well be endangered by a data loss. For most companies and organizations, losing correspondence with customers, customer contacts, electronic orders, production data, or other data essential to operations would be a disaster.

Although data security is essential for the protection of personal data and the privacy of individuals affected by data processing, this field of expertise is by no means limited to the protection of such data. Rather, data security measures serve to protect all data and information stored or processed in a data processing system.

The simple example of a damaged hard disk was chosen here to explain that data security is not only intended to prevent illegal activities by hackers. Rather, data security also aims to prevent the loss of data (with and without personal reference), the unintentional destruction of data, the unauthorized manipulation of data and the unauthorized disclosure or dissemination of data, as well as to provide protection against computer viruses, Trojan horses and malware.



Hazards in the Technical Environment

5

Abstract

In companies and organizations, servers and components of the IT infrastructure are often in operation around the clock. The stress on the material used is correspondingly high. It is therefore not unusual for defects to occur on such computers after a few years of continuous operation. However, there are many other hazards for servers and IT systems. This chapter provides an overview of the dangers to which servers and IT systems are exposed in the technical environment and how to deal with them. Practical examples are used to explain what should be avoided and how IT systems can be protected against certain hazards.

As discussed in the previous chapter, hackers are by no means the only threat to data and computing equipment. Water or sewage can cause severe damage to server rooms or computer equipment if a leak occurs or a pipe bursts. There are also other hazards that can occur in connection with water. These are, for example, flooding in the vicinity of rivers and lakes or heavy rainfall events. The threat posed to data processing systems by water is often not noticed until the damaging event has already occurred. A common saying in engineering circles is, “*Water always finds its way*”. Therefore, the worst conceivable place to build a server room or a data center is on the lowest floor of a building or in the area of an underground parking garage. Basements are often used to house server or telephone system because other spaces seem too precious to be used as server rooms. Figure 5.1 shows an example of such an obvious mistake: server, telephone system, and a

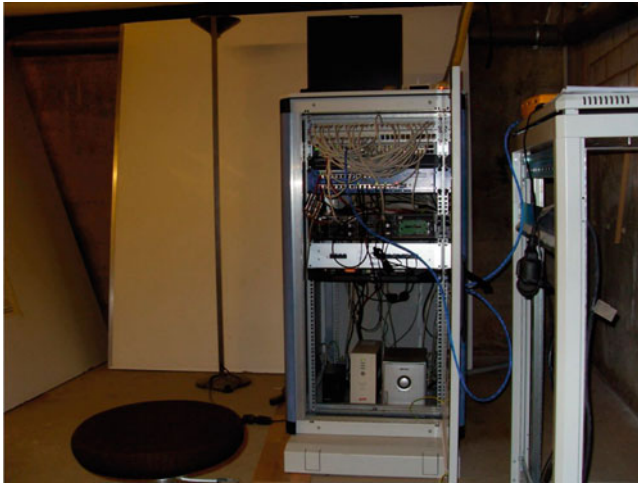


Fig. 5.1 A server cabinet in the deepest cellar of the building

network-attached storage (NAS¹) device used to store backups are located in a small server cabinet installed in an unprotected area in the lowest basement of a house. Unfortunately, what you can't see in this picture is a pump well about 120 cm deep located directly in front of the server cabinet. The presence of the pump shaft also makes sense in this basement, unlike the server cabinet, because there is a river about 30 meters behind the building that overflows its banks from time to time, especially after heavy prolonged rainfall. In the past, the pump shaft has therefore been used several times to pump out water masses that have penetrated the cellar. As already mentioned, such a basement is generally the worst place for the operation of electrical systems and equipment, especially computers and telephone systems. In the case described, there is no question as to whether water will damage the computer systems. Rather, the only question here is when the next flood will completely destroy the IT² and telephone systems. As soon as the water level reaches a depth of 30 cm in the basement, the uninterruptible power supply (UPS) and the storage unit (NAS) on which the data backups are located will be destroyed first. So, figuratively speaking, one of the most important and elementary measures

¹Network Attached Storage.

²Information Technology.

of data security and data protection dies first with the data backup. Since the uninterruptible power supply in the server cabinet is positioned directly next to the NAS, the power supply of the server cabinet will fail early. This means that both the telephone system and the computer network will then be out of service and the company will have the greatest difficulty in maintaining business operations. If the water continues to rise in the basement in question, it is likely that all computers and telephone system components located in this server cabinet will be damaged.

In order to cause the flooding of a basement or underground car park, it is not essential that the ground in the vicinity of the building is flooded. The groundwater level often follows the level of a river flood. Groundwater can then make its way through basement walls and floors and flood a basement even if no flooding is seen above ground.

Even if the base of a house is protected from flooding and a high water table, from a data security point of view there is not sufficient protection in the long term for the information and telecommunication systems operating in such a premises.

► **Note 1** *Avoid placing computer or telephone systems, especially server rooms or parts of data centers, in underground basements or garages. Such systems should be located in the middle of a building (BSI2016-1).*

Especially in connection with leakage and pipe bursts, it is important to think about a problem that occurs particularly frequently in older buildings. Insofar as renovation of older buildings is taking place or a server room is to be installed in such a building, it is not always possible to lay found pipes. In many projects, one is therefore confronted with the fact that water, waste water or heating pipes run through a room that is to be converted into a server room.

The best way to avoid compromising IT equipment is to decommission such piping or to be laid in parts of the building that cannot affect the server room in the event of a pipe rupture or leak. In many cases, however, decommissioning or decommissioning of such piping is not feasible. In such cases, only two alternatives remain: you can either choose a room in the building that is less at risk or install appropriate protective devices. As an example, Fig. 5.2 shows a sectional drawing from a project that depicts wastewater pipes running directly above a server cabinet. The area below has been protected by installing a stainless steel tray. If a leak occurs, the stainless steel tray prevents damage to the server room. However, such a stainless steel tray must then also have a drain (with siphon) and detectors, otherwise there could be even greater damage if the stainless steel tray is slowly filled by a leak and the anchoring can no longer withstand the weight. Although one might wonder what goes on in the mind of a planner who forgets to include a drain and

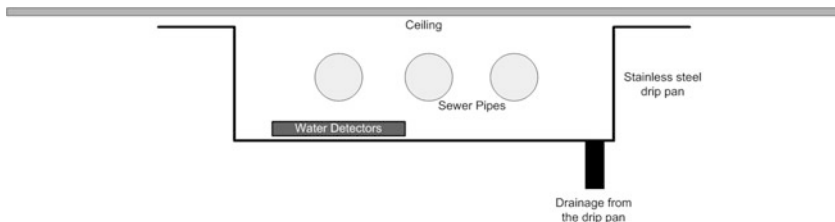


Fig. 5.2 A steel tray to protect IT equipment from pipes

water detector in a sump, it should be noted that in practice this is not even a rare mistake. Figure 5.2 shows a schematic representation of how such a collection tray can be mounted.

Finally, one should never overlook the fact that water also finds its way through ceilings and doors. A very popular method used by saboteurs is therefore to block drains and overflows and then turn on the corresponding taps. If no work is done in a company or institution at the weekend and the sabotage act is perpetrated in such a way that it is not noticed before the weekend, any reader can probably well imagine the extent of the damage to a company or institution. It would be beyond the scope of any publication to try to describe all the constellations of water hazards. However, you should be particularly careful in this regard if someone recommends that you install an air conditioning system in your server room that is operated with pressurized water.

Another serious and equally underestimated danger for data and data processing systems is fire. In case of fire, a well thought-out emergency plan and technical and organizational measures can ensure the survival of the company. If fire protection measures are implemented in a server room, then we protect the server room, as a mostly business-critical infrastructure, from the rest of the company. At the same time, however, we also protect company buildings and companies from dangers that could originate in the server room.

Those in any doubt that fire poses a real threat to data and data processing systems are strongly advised to seek advice from their fire safety officer or local fire brigade regarding this threat and its possible consequences.

A fire can not only break out in production lines, hazardous goods warehouses or in offices. A fire can just as easily break out in server rooms, in network distribution cabinets or even directly at a user's computer workstation.

This book is not aimed at theorists sitting in some university ivory tower thinking about probabilities of damage events just because data protection and

data security are currently “in vogue”. Rather, it is aimed at the practitioner and therefore also provides examples from practice and the author’s wealth of experience:

Due to the Sunday ban on trucks driving in Germany, a Saturday evening seemed to be the best time to perform a database migration within a large logistics company. During this time, the offices were unoccupied and the IT and database experts were the only people present at the company headquarters. While the system migration was being performed, a loud noise was suddenly heard in the corridors during the night, possibly indicating an explosion. Upon searching for the source of the bang, those present discovered a conventional CRT monitor in an office with smoke and flames already billowing from it. Apparently, an electrical component had exploded and started the fire. The fire was quickly extinguished. Without the coincidental presence of the IT experts scheduled for that day, the now aging main building of the logistics center would probably have burned down that night.

► **Note 2** *Terminal devices such as workstation computers, monitors and printers at the workplace should always be switched off when they are not needed (for example, outside office hours).*

Other fires were caused by defective power supply units or network distributors.

A fire can threaten the continued existence of a company. Especially if it takes days or even weeks to replace damaged equipment, install new cables (network, power supply) or if not only the server but also the server backup is burnt down, a fire in the environment of the IT systems of a company can lead to the bankruptcy of the same.

One of the most dangerous situations the author has experienced so far was caused by the cascading of several socket strips. Figure 5.3 shows the original situation just before a fire broke out. An uninterruptible power supply was available, as can be seen in the background of Fig. 5.3, but it was out of service because the batteries had been defective for some time and a repair had been neglected.

Most of the power strips and power cords shown in Fig. 5.3 terminate in the triple outlet on the front left, which in turn was connected to a standard outlet on the wall. When this picture was taken, the cable of this triple socket was already so hot that you could hardly touch it.

Improper electrical wiring can lead to more than just cable fires. Overloaded or unstable power grids can also cause damage to ITC³ equipment. Similar to water,

³Information and telecommunications equipment.

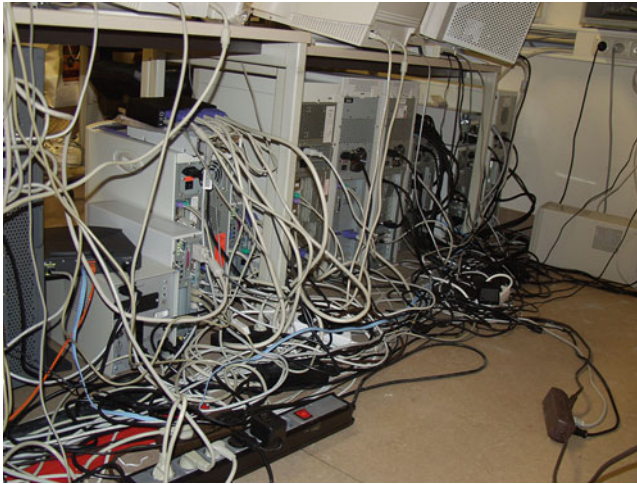


Fig. 5.3 Chaos in a part of a clinical “computer centre”

electrical currents also find their way. These are referred to as fault currents, which not only represent a problem for systems and equipment, but can also be life-threatening for the user of devices and equipment. For this reason, a regular inspection of electrical equipment is prescribed in Germany in accordance with DGUV⁴ Regulation No. 3 (formerly: BGV⁵ A3). In addition to computers and servers, this also includes other electrical devices of the IT and telecommunications infrastructure. In this regard, however, we refer you to further study of the corresponding regulation.

- **Note 3** *Avoid the use of cascaded sockets. The electrical supply of IT systems must be carefully planned by a specialist.*

Lightning strikes and electrical discharges are also a danger for IT systems. Therefore, the electrical supply of a computer system, a server room or a data centre must be protected against the consequences of a lightning strike.

⁴German Social Accident Insurance.

⁵Trade association regulations.

The phenomenon of lightning is an electrical discharge that can have a current strength of several hundred thousand amperes. Such a discharge can generate a magnetic field that can damage devices and magnetic data carriers.

The risk of lightning strikes and fault currents is often underestimated when computer networks are newly installed. Current network technology still largely uses copper cables in addition to fiber optic cables when new cabling is installed in buildings and on company premises. For one thing, copper wiring is a very good conductor of electricity, and for another, lightning does not distinguish whether it is affecting a power line or a network cable. Let's imagine a company whose computer network is secured in a variety of ways against Internet and other threats. To enter a company building or to enter the premises with a vehicle, it is necessary to identify oneself with an RFID⁶ token. Upon entry, a barrier opens after the RFID token has been successfully verified. For this purpose, the reader is connected by means of a copper cable (for example EN-50173-1⁷/category 7). During a thunderstorm, a lightning strike hits the open barrier system and the company's entire IT systems are destroyed in a fraction of a second. It is known from lightning damage to computer networks that even the metal contacts of network plugs (RJ45⁸) are vaporised in the process. However, a lightning strike can affect more than just electronic components or lines. Damage to equipment can also result in massive damage to databases.

Nowadays, no commercial enterprise can work without a database system. The spectrum of databases ranges from a simple address database to highly complex systems for production planning and control or ERP⁹ systems.

Databases are mostly very complex and equally fragile systems. When shutting down a server on which a database is operated, the database therefore first needs a controlled shutdown of its services. Otherwise, the database may be damaged and data may be lost. Such damage can occur, for example, if a sudden power failure occurs. For us, this means that we have just identified another threat to data security: The sudden and unplanned shutdown of servers. It is a fundamental requirement when operating servers, and especially when operating database servers, to protect

⁶Radio Frequency Identification.

⁷European Normative 50173-1:2011 about Information technology—Generic cabling systems—Part 1: General requirements.

⁸Registered Jack 45.

⁹Enterprise Resource Planning.

them from power outages, surges, and voltage fluctuations. To avoid defects in servers or in databases operated on them, it is therefore advisable never to connect the devices directly to the mains. An essential device without which no (database) server should be operated is the uninterruptible power supply (UPS). Such devices use accumulators to keep a server available even if the power supply is disrupted or fails for a short time. Uninterruptible power supplies designed for professional use often come with an interface and associated software. When battery power reaches a critical level due to the duration of a power outage, the software initiates a controlled shutdown of the server and its services so that no damage can occur to the data files or databases.

- **Note 4** *Never operate a server without protection by a sufficiently dimensioned uninterruptible power supply.*

Regarding the use of uninterruptible power supplies, regular maintenance should be mandatory (maintenance plan), as such a device can only protect a server and its data if it is working properly.

In this chapter we have seen that there are many more threats to data and computer systems than just hackers and viruses. In some regions of the world, it is even necessary to think about the dangers posed by earthquakes, landslides, hurricanes, or tsunamis.



Dangerous Software

6

Abstract

Dangerous software includes much more than just computer viruses, because the potential danger of a program does not necessarily correspond to the intention of a program developer. The chapter shows that the hazard potential of programs can have different reasons. The program may pose an intentional or unintentional threat. However, as will be explained further, a hazard can also result from a use of programs for a purpose other than that for which they were intended.

Software is sometimes no less dangerous than the threats discussed in the previous chapter. It is a popular saying, recited almost prayerfully by software developers, that bug-free software would not be available.

The reason why some contemporaries, most of whom work for software companies, repeat this statement over and over again is incomprehensible.

Maybe these people or the companies they work for are not very competent in what they do, or there are priorities set there that are against the development of qualitatively mature, well-designed and stable software. That means that it might not be wanted to develop bug-free software at all.

An example that actually happened will explain that sometimes the priorities of software companies prevent the development of high-quality software:

An experienced software developer moved to a well-known software company a few years ago. After a few weeks, the head of the development department had a look at the developer's screen while he was developing a new module for an ERP system. The development manager questioned him about the coding, which seemed "unusual" to him, and received the answer that he would write debug code so that logical errors as well as errors in the coding could be immediately identified and

corrected during development. In fact, he was programming according to standards and conventions that were already internationally accepted at the time. The developer was then told by the development manager to stop programming bug-free code immediately, because the company's goal would not be to "deliver high-quality software to customers" but to make a lot of money as quickly as possible. That same week, the developer left the company, which still sells ERP software to this day.

Even if, as is to be hoped, this company does not represent an entire industry, it must be assumed that there are other, different reasons why software can be faulty. For example, in some companies this can certainly be attributed to the high complexity of the systems or to the poor training of programmers and developers. In any case, the multitude of program errors that appear every day in a wide variety of software programs shows that, in general, we should not assume with more complex systems that software once purchased will also function perfectly. Program errors can lead to serious security problems on computer systems or corporate networks. In 2014, there was a worldwide problem that became known as the "heart bleed bug". The cause of this was a (preventable) programming error.¹

But what can we do about such security problems in software systems? We do not usually write our own programs or operating systems. So the only way we can do that is to regularly make sure that updates are promptly installed in the systems we use. As soon as a security problem is discovered in a standard software, the attacks, which want to use the known security gap, start shortly after. It is therefore essential to install system updates as quickly as possible and thus close any security gaps that are discovered. It should therefore be regularly checked whether security-relevant updates are available for the operating systems used or for application software.

► **Note 5** *Regularly check whether security-relevant updates are available for software or operating systems in use.*

Software, like other products, is subject to a life cycle. If we assume that an operating system is no longer supported by the manufacturing company, then we must assume that no security updates (so-called patches) will be available in the future. This means that if a programming error or a security problem is found after the end of the software life cycle, there will be no security update/patch available to close the corresponding security hole in the system. Therefore, there is a very high risk to the system and even data on such a server or computer if the operating system

¹<http://heartbleed.com/>. Accessed 12.01.2017.

is not further maintained by the manufacturer. For this reason, it is an essential requirement for the operation of secure IT systems not to use outdated operating systems, especially if the computer system is connected to the Internet.

► **Note 6** *Do not use an outdated operating system.*

Up to this point, we have only dealt with productive software systems. However, there are also numerous programs that have been developed to cause damage, spy on data, or support illegal or destructive activities. A selection of such programs is described in the following lines.

6.1 The Trojan Horse

Ancient Greek sagas and legends tell us how Odysseus deceived the Trojans with a giant wooden horse. The Trojans believed that the horse was a gift of peace and that the Greek fleet was on its way back. So the inhabitants of the previously besieged city pushed the horse into their fortified city and at night Greek soldiers jumped out who had hidden inside: That was the end of Troy!

For a certain type of malware, no other term would fit better than to call the programs Trojan horses, because these programs use exactly the strategy devised by Odysseus, pretending to be something other than what they actually are.

A common example of such a Trojan is email attachments, which are supposed to be telephone bills. If such a file is opened, a computer must usually be considered compromised, i.e. contaminated by viruses or malware.

Since powerful antivirus programs, which should be installed as standard equipment on every computer, usually find viruses attached to e-mails, the attachments do not always contain the virus that is to be distributed. Instead, it is possible that a connection to a server on the Internet is first established via the mail attachment and that viruses and malware are then loaded onto the computer from there. There are also known cases in which not even the last described activity is carried out directly. Instead, when the mail attachment is clicked on, some malware first makes an entry in the operating system's scheduler, which is then executed after hours, days or weeks and loads a malicious program or virus onto the infected computer. This can take the form, for example, of a URL address being addressed by the scheduler. The same processes can also be triggered by clicking on a link on the Internet. If a website promises you that you can download thousands of ringtones for your mobile phone for free, you should exercise caution. In this case, the probability

would be very high that you will install a virus on your device instead of the expected ringtone as soon as you click on a corresponding link.

In some cases, source codes or batch files are used as Trojan horses. For a savvy hacker, all it takes is one or two lines of code hidden in a script several thousand lines long. Perhaps the easiest way to break into a company's computer system is also the most ingenious:

An attacker does not have to look for security holes in the company's firewall. He does not even have to overcome this firewall and can prepare his attack at home without much effort or stress. All he needs is a program that allows him to gain access to a computer over the Internet. This program can be disguised as a document that pretends to contain, for example, a surveillance log or confidential management information. Very subtle is also the disguise as internal information of a competitor. There are no limits to the creativity of an attacker. The prepared Trojan horse is then copied onto USB² sticks and distributed in the parking lot of the company that is to be attacked. The finder will believe that someone has lost his USB stick. Unless the connection of unregistered USB sticks is technically prevented, the attacker is already quite close to his goal. The finder will in most cases, either out of curiosity or because as an honest finder he wants to return the stick to its owner, connect it upon arrival at his office. This would most likely make the attack on the company successful, because depending on how it works, the virus would install itself immediately when the stick is plugged in or when a file is clicked on in the system, possibly opening up access for our hacker to the infected system. Once a system in a company is infected, it can be used as a launching pad to attack other computers or servers within the company.

► **Note 7** *Never connect a found, unknown or unchecked USB flash drive or other removable media (DVD,³ external hard drive) to a production computer system.*

Finally, there are other ways in which a Trojan horse can enter a computer system. After the turn of the millennium, German investigative authorities used a Trojan horse to monitor computers connected to the Internet. This so-called federal Trojan horse was analyzed by CCC.⁴ It was able to monitor all components of a computer used for communication. In particular, the microphone, camera and

²Universal Serial Bus.

³Digital Versatile Disc.

⁴Chaos Computer Club.

keyboard could be monitored. In addition, the Trojan is said to have been able to monitor audio and video calls, and through this malware program, there was access to all data stored on the hard drive of an infected computer. However, a planned widespread use of the program was prevented by the highest court. Nevertheless, such malware programs are said to have repeatedly appeared on computers, especially on mobile computers. Even if German investigative authorities nowadays only use the federal Trojan within the scope of a legally permissible deployment, this does not mean that similar legal barriers to the use of such a program have been erected in other countries.

It is not unlikely that such malware will also be installed on mobile computers at foreign airports when notebooks or tablet PCs are transported in checked baggage and not carried as hand luggage.⁵ It is also very popular to install a Trojan when computers are left behind in a hotel room, for example, while the owners are having dinner or attending a social program at a conference. The attacker then has access to the device as soon as it has established a connection to the Internet.

There is no significant difference between the techniques and malware used by government agencies and services and the malware used by criminals and spies when it comes to remote access to computers.

Some computer users still think that the data they store on their mobile computers would be safe because a password is required to log in to the device. In order to infect a notebook computer, the system does not need to be started, nor does a successful logon to the operating system need to occur. Someone who wants to infect your notebook in the company or in a hotel, for example, will not start it. It is often sufficient to loosen just one screw on the underside of a notebook to be able to remove the hard disk. The hard drive is then connected to another device, infected and put back into the notebook. This procedure takes no more than two minutes. But how can you defend against such an attack? It is much more difficult to infect a computer using the method described above if the hard disk is fully encrypted. In this case, connecting to another device would be useless in the first place, because without the appropriate key or algorithm, data on the hard disk cannot be accessed, which includes write access.

⁵ See Frank Rieger, Ein amtlicher Trojaner - Anatomie eines digitalen Ungeziefers, Frankfurter Allgemeine Zeitung (09.10.2011), <https://www.faz.net/aktuell/feuilleton/ein-amtlicher-trojaner-anatomie-eines-digitalen-ungeziefers-11486473.html> Accessed 27.07.2021

- **Note 8** *If sensitive data is stored on a mobile device, encrypt media or data using the best method available and do not leave the device unattended.*

To make it easier to identify tampering with the notebook, it is useful, for example, to secure the screws of the hard drive mounting tray with adhesive seals that can only be removed by destroying them. Although this measure cannot prevent the illegal action, a destroyed seal provides the information that a computer may have been compromised.

After the previous explanations about the use of Trojans, the question now arises: how to identify a connection between a computer and any server on the Internet? The answer to this question is surprisingly simple.

If a Microsoft operating system is installed on a computer, the “netstat” program is available within the command shell (cmd). This tool provides an easy way to search for open connections of a computer or to display ports that are waiting for incoming connections. All you need to do is enter the following command:

```
netstat -a
```

If you add the “-b” option to this command, you will also receive information about which service or program has established a connection or is expecting one. If the result provided by the program does not tell you which server has established a connection with the examined computer, you can use a search engine to look for its IP address.

However, as easy as the program is to use, such an investigation can be tedious. Typically, a large number of programs establish connections to the Internet. First of all, e-mail programs, for example, connect to mailboxes on servers on the Internet. Then, of course, browsers establish connections to the servers on which the accessed Internet pages are stored. Finally, connections are established to update antivirus systems, to check the licenses of some software systems at startup or during runtime, or to inform the user about available software updates.

So if a query with “netstat” returns an extensive list of connections, it does not necessarily mean that a machine is infected. When examining the output of this program, the approach should be to check each connection and look for anomalies or unknown connections or reasons for connections. Particular care should be taken, as some malicious programs deliberately use similar names to programs that make legitimate connections. In some cases, the difference may lie in one letter or an otherwise minimally altered spelling, which the observer may miss when quickly looking through the program.

However, every user of the “netstat” tool should be aware of one limitation. The program only provides a snapshot. If a Trojan does not permanently attempt to establish a connection to an Internet server, but establishes connections on a time-controlled basis, it is possible that it does not appear in the query with “netstat” at one moment and establishes a connection to its server again at the next moment.

If the network under consideration has a firewall that is designed for professional use, a so-called monitoring tool is often available. This makes it possible to analyze snapshots as well as connection data from the past and to identify established connections or connection attempts. Such a firewall should not only be maintained and updated regularly. A connection check should also be carried out regularly, which is designed to identify Trojan horse connections or other illegal or unwanted connections between a computer or computer network and the Internet.

6.2 The Virus

Comparable to a biological virus that infects people unnoticed, a computer virus is also invisible during the process of infecting computers. The way a computer virus works can be very different. Viruses can be classified firstly by the route by which they spread and secondly by what activities they perform. Accordingly, the components of a computer virus can also be distinguished between means of transport and payload. The means of transport is the way the virus uses to enter a system. The payload is the program that is executed after the virus has infected a computer. Neither parameter is limited to single methods. A virus can spread through a Trojan horse, through vulnerabilities and security holes in operating systems or programs, through external storage devices, or via email. There are almost no limits to creativity in this respect, and it is often the case that malware is loaded onto a computer and activated there by the active actions of the user. More information on this topic will follow later.

The range of activities that can be performed by viruses is also almost unlimited. Two of the oldest known viruses are called “stoned virus” and “autumn leaves”. The action of the former was limited to outputting a message on the screen, which demanded to legalize marijuana.

The second virus caused letters of displayed text to virtually fall down the screen, as if a tree were losing its leaves in autumn. What seems rather amusing today, however, was an early warning that we could lose complete control over our data if the new technology were to evolve and be used unthinkingly.

Today, the activities of viruses are not nearly as harmless as they were in the early years of personal computers and the Internet. Viruses are now used specifically by criminals to steal data from credit cards or bank accounts, for example, or to gain access to personal data. However, viruses are not only used by ordinary criminals. They are used for espionage and sabotage, and some have been used to damage critical infrastructure such as nuclear facilities. Some viruses and malware have enormous destructive potential.

So-called Bot viruses are used to hijack private computers or company computers and use them as part of their own network for criminal activities. Viruses are a constant threat to companies, national and international economies, and public safety.

In practice, self-appointed computer experts, most of whom seem to be a sad remnant of a new economy, shock us time and again with statements about security programs that fundamentally call their use into question. Even today, IT security is still suffering from these excesses in the IT industry, which fortunately failed a few years ago. Competence had to give way to sheer and unlimited greed in a hype that we can hardly imagine in its dimensions today. So it is hardly surprising that even today, in software systems, infrastructures, but also in the heads of some consultants resistant to advice, legacy from this time can be found, which definitely carry a potential danger that can massively damage a company.

Letting a computer communicate with the Internet without special protection programs (firewall, AV⁶ program, etc.) can best be compared to jumping into a pool in which several hungry great white sharks are swimming around, right after you cut your finger. Anyone who still thinks that nothing can happen or that antivirus programs only serve the purpose of generating high revenues for the manufacturers should not tinker with IT systems in a professional environment.

It may well be an asset for many users and operators if an Internet connection is available on every computer in a company. However, the most effective way to fight viruses is to prevent them from spreading. This raises the fundamental question of why every employee in a company needs a connection to the Internet on their computer. Even further questions arise in relation to critical infrastructures. Why do the computer networks of a nuclear power plant, a company's research and development department, a hospital operating theatre and a military headquarters need to be connected to the Internet?

The Internet was originally a military invention. In the meantime, however, it has developed into the World Wide Web, which is available to everyone and is thus also

⁶ Anti-Virus.

available internationally to every secret service, every terrorist organisation and every criminal gang.

Do you really want to expose yourself to the dangers of this network and, when protecting secrets, patents, information or assets, hope alone that system updates will be applied to a company's firewall and antivirus server in time before a newly discovered security hole is exploited by an attacker?

It is possible to effectively protect yourself from computer viruses.

Some companies have developed concepts that completely decouple internal networks, in which sensitive data is processed, from networks that provide access to the Internet. Furthermore, in such internal networks, the use of mobile devices and storage is prevented by technical measures. If, however, there is no longer any possibility for a virus to penetrate a network because it cannot reach it either via a LAN connection or via external data storage, this network cannot be infected. This would also make it inaccessible to hackers.

More often than networks that are completely separated from the outside world, however, hybrid solutions will be found in practice that, with the use of extensive security precautions, for example, allow the updating of a virus program, but otherwise do not allow any connections to the Internet.

Since new threats or new versions of malware appear on the Internet almost every day, it is important to use professional antivirus systems that automatically check for updates at least once a day.

Some system houses still exclude the use of antivirus software on systems that are supposed to run programs distributed or developed by them. Do not put your company's existence at risk just because the developers of such a company are unable to deliver properly functioning software. In general, you should not use application software that precludes the simultaneous operation of antivirus systems.

- ▶ **Note 9** *Don't let anyone touch your computers with the opinion that you don't need antivirus programs or firewalls.*
- ▶ **Note 10** *Do not connect critical infrastructure to the Internet.*
- ▶ **Note 11** *As soon as a computer is connected to the Internet, it is essential to protect it with professional security software and adequate hardware, and to update the systems regularly.*

6.3 The Logical Bomb

Such a malicious program—it can also be an executable script—can best be compared to an intelligent anti-tank mine, which only explodes when several criteria are met. But once it explodes, it leaves destruction and chaos in its wake.

Such a program can use a wide variety of ways to spread. Once it is active in a system, it can unleash its full effect at a predefined time or when a certain constellation occurs. In IT circles, it has been rumored for years that the use of logical bombs is particularly popular with IT administrators. It is very easy to build a logical bomb and usually such a bomb in a system is not detected by an AV program or other security software. The following example describes a case in which such a logical bomb was used by an administrator:

The IT administrator of a company was—for whatever reason—in dispute with the managing director. The system administrator saw himself as a victim of his boss's arbitrariness and feared being fired at the next opportunity. In this situation, he wrote a program, compiled the code,⁷ and installed the program in executable form on several of the company's servers. At first, the only activity of this program was to check once a month to see if the administrator's email account was still active. Then, after several months and the continuation of the skirmish between the boss and the administrator, the latter was fired. After a few days, his email account was deactivated and after another three months, it was completely deleted. It was this very deletion that now activated the logic bomb. The program started a "countdown" and after about a year, the program started writing memory junk, i.e. unallocable contents of memory, to randomly selected system files, deleting some files and directories, then deleting itself and restarting the respective systems.

► **Note 12** *Never get into a dispute with your IT administrator. If you are forced to fire him, do not hesitate for a moment and change all relevant passwords and access codes immediately.*

Such attacks from within a company or organization are extremely dangerous, especially since we would usually only expect attacks on our systems from the outside world. Theoretically, the administrator in the example described could also have sabotaged the data backup, which would then have led to systems and data no longer being able to be fully restored.

⁷Translation of the programming code into executable machine language.

Because a company's employees typically need access rights to systems and access rights to data and information in order to perform their job duties, it is much easier for employees to steal data or manipulate or sabotage systems than it is for outside third parties.

6.4 The Keylogger

A keylogger can enter a system in the same way as a Trojan horse or a logic bomb. Therefore, it is more important to think about how this malware works. A keylogger is a special kind of data collector. It collects all the input that is made on the keyboard. It does not matter what programs are used on the computer or what purpose is served by the computer usage. The keylogger logs every message and every command directly when it is entered via the keyboard. This not only makes it possible to obtain passwords for all software systems used on an infected computer; a keylogger can also store data before it is encrypted or transmitted through encrypted connections. Some keyloggers are able to connect to a server on the Internet and send the information collected in the computer there.

6.5 The Sniffer

A sniffer⁸ is a program that monitors network traffic and provides insight into the transmitted data packets. It is primarily used for network troubleshooting, but can also be used, as the name suggests, to illegally obtain data. At this point, the reader is requested to use such software only for legal purposes. As we have already seen in Chap. 3, communication within networks is described by the OSI reference model. Sniffers can log very different parameters. For example, a packet sniffer can log all TCP packets (OSI layer 4). Within these packets are messages and data transmitted over the network. As long as the network communication between two computers is not encrypted, messages in TCP packets can be found and read logged as plain text.

Even queries to databases and their results can be read in TCP packets. Figure 6.1 shows a screen shot of the program Wireshark, one of the most commonly used tools for network analysis. It can also be easily misused for spying data in the context of criminal activities.

⁸Software for spying on data.

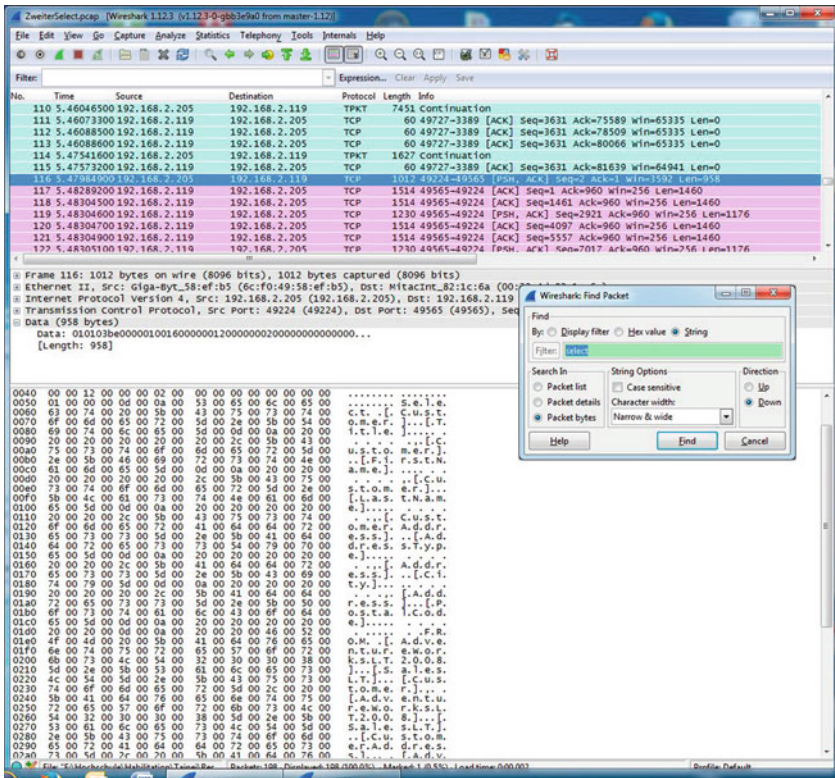


Fig. 6.1 Wireshark analyzing database queries

But now the question arises how it is possible to spy on data with such a tool. A few years ago, it was much easier to read the data traffic in a network, because in the late 90s of the last century, many networks used so-called hubs to supply the individual network connections. Today, instead of hubs, switches are used and their use is now standard. Both devices are network distributors, although only switches are likely to be state of the art today. Hubs did not know on which port⁹ of the device a particular computer was connected.

⁹Port is used here in the sense of connection and must not be confused with the port of socket addressing.

Therefore, each data packet transmitted over the network was sent to each of the active ports of the hub. This also made it possible to log the complete data traffic within the network at each port of the hub. The switches (network distributors) used today are intelligent devices. This means that these devices learn which computer or other device is connected to a particular port on the switch. The switch learns the structure of the network as it operates. If the switch now knows which device is reached via a specific port, then data packets for the corresponding target computer are also only routed via this port. This makes it much more difficult to log the complete data traffic within a network. However, if the hacker has access to a configurable switch, he can define a monitoring port there. This is actually only intended for administrative purposes and for analyzing network problems. However, if a port is defined as a monitoring port, all data packets that pass through the network distributor are forwarded to it. In this way, complete network infrastructures can be manipulated in such a way that a copy of the entire data traffic of a network arrives at a specific port of a selected switch. However, such a case is only possible if the hacker also has physical access to the monitoring port. If the network distributors are not sufficiently secured by passwords and all network sockets, i.e. also those that are not required or are located in publicly accessible areas, are connected, then it is possible for an attacker to gain access to the network and access to the network distributors via a connected network socket and to set up the used port accordingly.

The easiest way to sniff data is to have access to a main network connection, such as the line between a central switch and a firewall. If all traffic between the corporate network and the Internet passes through this firewall, or through the line between the central switch and the firewall, it is fairly easy to install a sniffer computer and record all traffic to the Internet.

All we need is a computer that has two network cards. These two network cards are configured as a bridge. This means nothing other than that all data between the company network and the Internet is only routed via the bridge. This is usually not visible to the user. On the PC, which now literally has to endure all communication with the Internet, every data packet can now be logged without exception. In this case, all data packets can be written to a sufficiently dimensioned hard disk and are available for later analysis.

An example of the legal use of such a tool, including the bridge described, is easy to follow.

As part of a project, an IP-based telephone system was put into operation in its own network segment. The workstation computers were located in another network and a CTI solution installed there was to communicate with the telephone server via the firewall located between the networks. While the telephones were also located in

the network of the telephone system, so-called head-sets were installed on the computers on which the CTI software was used. After commissioning, telephones could call the head-sets, but the voice was not transmitted when the call was accepted.

So data packets were recorded on both sides of the firewall. Wireshark has the ability to reassemble the data packets into complete phone calls. These can then be listened to if the appropriate loudspeakers are attached to the computer. In this case, no voice packets actually arrived in the CTI network. The firewall ports required for communication were then checked. Finally, a malfunction in the software of the telephone system was identified, which could then also be remedied.

The example from 2016 shows how sniffers can be used sensibly. But it also gives an idea of what such tools can do in the wrong hands.

Just like the recording of the complete data traffic, the complete telephone traffic can also be recorded if the company works with Voice over IP technology. Therefore, it is an essential measure that access to switches, firewalls, routers and gateways is blocked for third parties. Unfortunately, in practice one repeatedly encounters scenarios in which telecommunications lines and Internet connections in the unlocked basement of a company building are accessible to any attacker.

A sniffer can also work with filters so that only selected data packets are recorded. For example, the IP address of a specific computer can be used as a filter if this computer is causing problems with network communication or access to the Internet, for example. The sniffer will then only record the data packets that are exchanged with this computer. This makes the amount of data to be analyzed later much more manageable. Another example of the use of a sniffer is the analysis of SQL queries for the later use of technologies and methods from the areas of data warehouse and business intelligence.¹⁰

What can be done to protect against attacks with sniffer programs?

On the one hand, it must first be pointed out with regard to this question that sniffers are required in the vast majority of cases to find problems in complex networks and are indispensable in this regard. Therefore, such tools belong to the standard repertoire of administrators. As mentioned before, an essential measure against illegal sniffing¹¹ is to secure the access to technical rooms and especially to server rooms of a company. It is essential to prevent unauthorized persons from gaining access to computer systems. Some corporate computer rooms are secured like Fort Knox or the Bank of England. However, somewhere in the

¹⁰ Analysis of economic data of a company.

¹¹ Data acquisition by means of a sniffer software.

unsecured basement of the building you will then find—as mentioned above—telephone lines, telephone distributors, telephone systems, internet routers and other communications equipment. You really can't make it any easier for a hacker.

- **Note 13** *Prevent any possibility of access to computer systems, network components and central communications equipment, especially firewalls and routers, by unauthorized persons.*

6.6 The Back Door

The English term “backdoor” is commonly used internationally in computer science. The original purpose of this method in connection with computer systems was the intention of many developers or system administrators to have an always available access to a system in case of emergency. Today, the background for a “backdoor” can also lie in the inability of developers that results in poor or faulty coding, which then enables an attacker to break into a system. So today this term stands for both a planned and an accidental possibility to gain access to a system in a non-regular way. To find such backdoors, hackers usually analyze the coding of a system. In the past, programmers sometimes built a backdoor into the kernel of an operating system. The core, or kernel, is the basic framework of any operating system. In an older Unix system, it was possible to obtain maximum rights to all data, programs, and functions by adding a simple password as a parameter to the command line during the boot process.¹² It cannot be ruled out that even modern operating systems still have backdoors. It is therefore not sufficient to rely on assurances from software manufacturers. Therefore, protective measures that go beyond the capabilities of an operating system should be mandatory in the area of professional computer use.

- **Note 14** *Never rely solely on the alleged security of an operating system.*

¹² Booting the computer and loading the operating system.



Removable Media, USB Devices, Smartphones and Other Mobile Devices

7

Abstract

USB sticks and other mobile data carriers have become indispensable in the daily use of IT systems. Yet these media are usually handled quite carelessly. One possible reason for this could be that the dangers of this technology are generally underestimated. This chapter therefore describes the basic dangers for IT systems and data through the use of mobile devices, external data carriers and smartphones.

USB hard disks and especially USB flash drives have achieved an impressive capacity and high data throughput in recent years. Today, they are indispensable components in the world of computers. Since removable media are now used almost everywhere, people hardly think about potential dangers when using this technology. These mostly overlooked dangers can be very diverse and range from virus infections to espionage. If we recall an incident related to Wikileaks, thousands of files and documents were published that a former Pentagon¹ employee simply copied onto a USB stick and took with him. In the past, espionage cases have also repeatedly become known in which infected USB sticks were used. The principle behind this is simple and at the same time efficient that one can confidently assume that hacking with USB sticks is the simplest, but by no means the most unsuccessful variant of breaking into networks. In doing so, the hacker takes advantage of human curiosity. Let's assume that a spy or hacker wants to break into a corporate network or the network of a government agency from which access to the Internet is possible. Then he can distribute used USB sticks infected with a

¹US Department of Defense.

Trojan or virus in the organization's parking lot early in the morning. The further progress of this method has already been described in Sect. 6.1. However, anyone who now thinks that an antivirus program would thwart the success of this attack would be best advised to read on first, which is described in the following case study:

In a case in which the author himself participated as a crisis manager some time ago, a representative of a company that manufactures medical devices visited the head physician of a medical department of a clinic. Before the chief physician was even able to explain to the representative that the use of USB sticks would be prohibited in the clinic, the representative had already connected such a device to a computer in the clinic in order to start a presentation. This USB stick was infected with a virus that was the latest derivative of a class of particularly dangerous viruses. The virus was capable of blocking antivirus systems and within a few seconds had already infected the clinic's entire radiology information system. However, the damage was not limited to this comparatively small network. The virus was able to use an open port in the firewall, which had to be open in order to view radiology images from the hospital's network. It only took a few minutes for the virus to infect the clinic's main network. The clinic information system, the laboratory information system and other central systems were now also affected. In total, more than five hundred computers and servers had to be cleared of viruses. The damage caused by the representative presentation amounted to about 300.000,€. At that time, the clinic was well equipped with firewalls and antivirus programs. E-mails were even scanned by three different antivirus systems. Despite all this, security measures were able to be improved even further. After the incident, administrators installed a system that blocked any unauthorized USB device on the entire computer network and set off an alarm if anyone tried to plug one into a computer at the clinic. Although every employee at the institution knew that the use of removable media was strictly prohibited, there were several alarms every day in the weeks and months that followed. Some of the employees wanted to work on private documents during working hours. Others complained that they were not able to show holiday pictures to their colleagues or that it was impossible for them to work on applications for other employers during working hours. The users' behaviour here lacked any awareness of injustice. Even if the case described only resulted in relatively manageable monetary damage, it shows that it can certainly end in disaster if the management of a company or the management of a public authority assumes that employees will adhere to specifications and prohibitions without restriction. The example also shows that in a professional environment it is not enough to use an anti-virus system to prevent problems caused by external data carriers. Especially in

areas where sensitive data is processed, it is essential to implement a technical solution that prevents the unauthorized use of external data carriers.

- **Note 15** *Use a technical solution to prevent the unauthorized use of mobile data carriers.*

If this chapter uses abstract terms such as mobile data carriers or mobile devices, these explanations naturally also apply to smartphones. Today, such phones offer the same range of functions as a portable computer and can be used as an external data storage device in the same way as a USB stick. This makes them suitable for spreading viruses and Trojans in the same way as USB devices.

Sometimes it makes sense to use USB sticks. However, it should be avoided that employees use private USB sticks. Instead, USB sticks should be purchased by the company if required and managed by the company.

The smaller the data carriers are, the more likely they are to be lost at some point. For this reason, sensitive data should not be stored on a USB stick as a matter of principle. To the extent that it is necessary to store such data on a USB device, there are special USB sticks that use state-of-the-art encryption. Some of these devices will erase all data on it if an attempt is made to open the case or otherwise tamper with it. When using such a data carrier, which is also available as an SSD, it can therefore be ruled out that data can be viewed by unauthorized third parties in the event of theft or loss.

- **Note 16** *If it is necessary to store sensitive data on an external/mobile device, use only devices with sufficiently strong encryption or store pre-encrypted files on a device.*



Telephone Systems

8

Abstract

While the tried and tested telephone network is gradually being replaced by the new VoIP technology, it is unfortunately very rarely made clear that the use of so-called Internet telephony also entails massive risks. For this reason, VoIP telephone systems are often operated without adequate protection. This chapter explains, using concrete examples, what the dangers of using VoIP telephone systems can look like and how one should protect oneself from the corresponding dangers.

The telephone has long since become an integral part of everyday work in a company. Many companies now use telephone systems that work on the basis of the Internet Protocol (IP). This form of telephony is commonly referred to as VoIP technology. VoIP is the abbreviation for Voice over IP. The voice is digitized and transmitted via ordinary Internet communication. The fact that telephone systems are connected to the Internet makes them increasingly interesting for hackers. These hackers attack the often poorly secured telephone systems via the Internet. Once they have penetrated such a system, they begin to set up connections with exorbitantly expensive, chargeable numbers in the Middle East or the South Pacific.

Obviously, technical progress also brings new problems. As long as telephone systems were not connected to the Internet, they could be operated relatively securely. Now, however, due to the use of new technologies, telephone systems are increasingly exposed to attacks from all over the world. In the meantime, such attacks have become the rule rather than the exception. In many cases it is even frighteningly easy to break into a telephone system via the Internet, as factory

passwords are often not changed during commissioning. In other cases, ports are not sufficiently secured and can be used to gain access to the systems.

What are the possible consequences of criminals gaining access to a telephone system?

In the best case scenario—whatever that means if the system has been hacked—a break-in into the telephone system will only cost a company a few thousand euros.

Typically, hackers then initiate phone calls to some very expensive phone services. In one case, the attack was carried out over the weekend and discovered on the following Monday. The damage caused “only” amounted to around 25,000 euros. However, if such an attack is not identified immediately, the damage can be significantly higher and may well be in the six-figure range.

But why should this be the most favorable case in which a company loses money? Well, in the case described, the company fortunately only lost money. If a telephone system is integrated into the company network, a successful attack on the system means that the hacker has already penetrated to a server (telephone system) in the middle of the company network. In this case, a telephone system can then serve as a starting point to attack other systems of the company. For example, settings from a production line could be manipulated, patents and technical instructions could be stolen, or other destructive activities could be carried out. Such an attack could potentially pose a massive threat to a company’s existence. Up to this point, we have only thought about companies in this regard. There could well be even more far-reaching consequences if not a production plant but a government agency, a country’s defence ministry or a nuclear power plant were attacked in such a way.

How can we protect ourselves against attacks against telephone systems (VoIP)?

A VoIP telephone system must be secured in the same way as all other computer systems in a company that are connected to the Internet.

This means nothing other than that such a system may only communicate with the Internet via a suitable firewall system. The configuration of both the telephone system and the firewall should be carefully planned.

Many modern telephone systems support CTI¹ solutions. These systems often link the contact data of office programs with the possibility of starting a telephone call via a mouse click on the computer and dialing a number accordingly. Such a link between the workstation computer and the telephone system can make an important contribution to making processes and workflows more efficient.

¹Computer Telephony Integration.

However, this also requires a connection between the computer network and the telephone system.

We should accept that telephony and computer networking represent fundamentally different technologies, even if they use the same protocol (TCP/IP).

Given the enormous risks posed by telephone systems connected to the Internet, it is therefore strongly recommended that telephone sets or telephone systems never be directly integrated into the computer network of a company or institution.

► **Note 17** *Never integrate telephone components into the computer network in which your servers and clients communicate.*

But how can a company work with CTI without running these different technologies in a logical network?

The answer is quite simple: As explained earlier, a telephone system should not communicate with the Internet without a professional firewall. A firewall can be configured to work with different networks.

One of these networks is the Internet. The second network defined in our firewall could be the communication network where telephones and the telephone system are installed. Finally, a third network can be set up in the firewall to accommodate the company's workstations and servers. Of course, some readers will notice at this point that proxy servers are sometimes housed in their own network segments. However, for the sake of simplicity, this circumstance will be omitted here. If, in the constellation described, an attack on the telephone system were to occur and be successful despite the protection via the firewall, the computer network would still be protected, since it would require another overcoming of the firewall in order to be able to attack the servers located there.

Nevertheless, despite the separation of the networks by the firewall, we can use a CTI solution, since it is possible to establish communication between the networks via precisely defined ports. For this purpose, access rules are set up in the firewall. By means of these access rules, only those ports are released for communication that are really necessary so that, for example, the CTI solution used can function without errors. The corresponding rules can not only control which ports may be used. They can also be used to determine which computers are allowed to use certain ports. The release of ports should always be done according to the minimum principle.

► **Note 18** *Never open more communication ports and connection options in a firewall than are absolutely necessary for planned connections.*

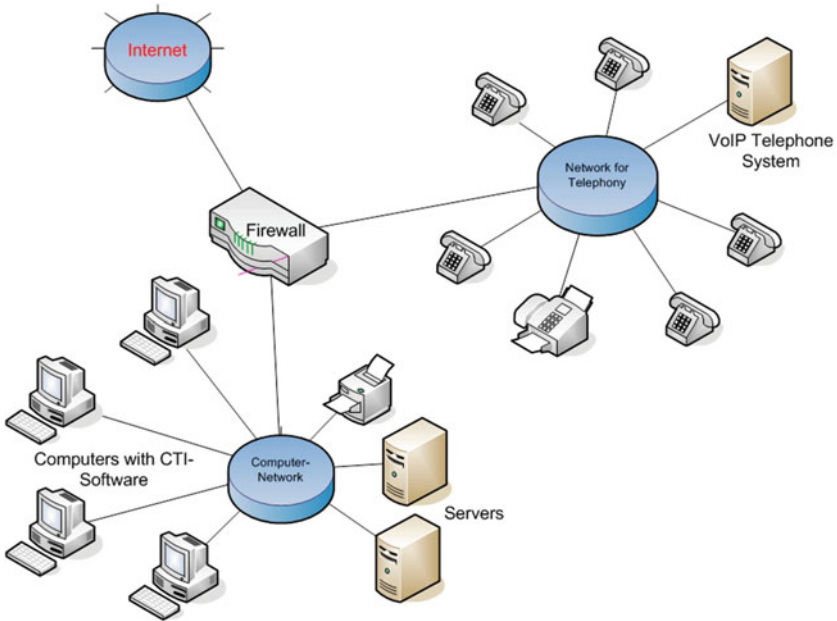


Fig. 8.1 Separation of IT and telephone network

Figure 8.1 gives an abstract overview of how computer networks and telephone networks should be separated by a firewall.

However, even if we achieve a decidedly high level of security through a well-configured and professional firewall, and other security measures, it is necessary to weigh up whether any residual risk is acceptable. If the computer network contains highly confidential information/data or if it is part of a critical infrastructure, such as a nuclear power plant, then there should never be a connection to a telephone system that is connected to the Internet. In critical infrastructure, anything that could cause a security problem now or in the future must be avoided. The optimal solution for critical infrastructure is to not be connected to the Internet.

- **Note 19** *Never connect a critical infrastructure to the Internet or to a telephone system that has an Internet connection.*

Since it is fundamentally necessary to secure a telephone system with a connection to the Internet in the same way as computer systems, it is also necessary for such a system to be regularly updated with security updates. To conclude this chapter on the dangers posed by telephone systems, it should be pointed out once again how easy it is to record, reconstruct and listen to telephone calls made using VoIP technology. In Sect. 6.5, which deals with the topic of sniffers, corresponding issues have already been addressed. This requires appropriate software, which is usually available free of charge on the Internet. In addition, a computer is required. This computer does not need any powerful components. It only needs to have two network cards with RJ45 connection and be equipped with a current operating system. If a hacker or spy gains access to the room of the company or institution where the router for Internet access and VoIP of this organization is placed, it is extremely easy to record all the data exchange of the organization with the Internet. The rest of the procedure has already been described earlier. In principle, such activities are conceivable at every important network node.

The author does not want you to get into trouble. Therefore, please use the methods described here only for legal purposes. Ensure that no unauthorised person has entry or access to your organisation's information or communication systems. The realisation of this requirement means that all rooms containing essential computer systems or telecommunications equipment must be adequately secured.

- **Note 20** *Protect all components and devices of computer and telecommunication systems against unauthorized access and unauthorized use.*



The Greatest Danger in a Digitalized World

9

Abstract

Data security starts in people's minds. Those who cannot imagine the damage that can be caused by inadequate precautions to protect company data may be inclined to handle data and systems carelessly. The chapter explains that data security is not exclusively a question of the technology used, but also requires responsible action on the part of employees.

The digital world is threatened by many dangers. The previous chapters have described some of these hazards that can threaten IT systems. These include fire, water leaks, lightning, technical problems, viruses, logic bombs or attacks by hackers or saboteurs. By far the greatest threat to the digital world, however, is the human being,¹ and in particular the employee or a member of one's own organization.

Sometimes even the administrator or the IT manager himself can be the biggest threat to a computer system. The following explanations will support this thesis.

Let us first take another look at the Wikileaks affair. The publication of secret documents is in no way to be judged in this book. Rather, we will look at the facts of how the affair came about in the first place: a soldier who was employed in the US Department of Defense copied thousands of documents, some of them secret, onto a USB stick and onto a CD-ROM, which, according to the labeling, was supposed to contain music videos. He left the building with the captured data and uploaded it to the Wikileaks servers a short time later. That was actually the whole story. It is not

¹Muench, Technisch-organisatorischer Datenschutz, 4th edition, DATAKONTEXT, Heidelberg, 2010, (p. 202).

essential for the consideration in the following what the motives for this action were. It is only relevant what happened here. This case can certainly be viewed from several angles. However, it proves that employees can be a pervasive threat to data security. In the facts described, there was an individual who was not loyal to his employer (US Department of Defense). However, there were also individuals who clearly did not do their jobs diligently.² In 2009 and 2010, there were already methods that could have technically prevented the copying of the data. However, the persons responsible for IT security failed completely with regard to transfer control and the prevention of unauthorised access to files. This made data theft much easier or even possible in the first place. In other words, the entire Wikileaks affair is entirely due to human error.

However, human error does not only manifest itself in such a sensitive environment.

Friedrich Nietzsche coined through a publication of 1878 with the title “Human—All-too Human”, a saying that has not lost its relevance until today. For the area of data security, this means that human influence must be seen as an essential quality factor of data security. In this context, a variety of human shortcomings must also be reckoned with, which include in particular ignorance, imprudence, dishonesty, lack of loyalty and unreliability.

In the same year that the Wikileaks affair happened, even small and medium-sized businesses in Europe were already equipped with software systems that triggered an alarm if someone tried to connect an external hard drive or USB stick to a computer on the company network without proper authorization.

It is astonishing that in the rarest of cases employees show a guilty conscience when they are caught in such actions, which are highly dangerous for the company.

So we should confidently assume that in at least every medium or large organization there are employees who do not care in the least about the security of IT systems or data.

How can we deal with the greatest of all threats to data security?

First and foremost, it is necessary to train employees with regard to system security and to sensitize them to the concerns of data protection and data security. In addition, it makes sense to oblige employees to comply with company rules and to instruct them about the possible consequences of violating service and procedural instructions. As far as possible in the company or organization, employees should be involved in the development and implementation of security concepts.

² see <https://www.dallasnews.com/news/news/2010/11/30/wikileaks-suspect-believed-to-have-used-cd-memory-stick-to-get-past-pentagon-security>. Accessed 27.07.2021.

But even a single employee who does not comply with data protection and data security requirements can cause considerable damage to the company. It is therefore necessary to implement all the necessary technical protective measures and keep them up to date at all times.

- ▶ **Note 21** *When it comes to data security, don't trust that employees will comply with the company's policies.*
- ▶ **Note 22** *Access rights should be comprehensively documented. No employee may have more access rights than they need to fulfil their operational duties.*



Abstract

In 1970s spy movies, documents regularly self-destructed after they had been read because no longer needed to be stored. Unfortunately, the reality is that many systems over the past decades have been designed and programmed to store data. For a long time, it was considered a mark of quality for archival systems that they were incapable of deleting or modifying data once it had been stored. However, today's legislation, at least in the European Union, requires that data relating to individuals must be deleted when the purpose for storing it has ceased to exist or a legal retention period has elapsed. In addition, there are a number of other reasons why data must be deleted. This chapter describes the problems that can arise when deleting or destroying data and provides appropriate solutions.

So far, we have considered what can happen to our data assets. In this chapter, however, we will not deal with accidents, accidental destruction, or computer sabotage. Rather, we will now look at destroying data intentionally and willfully, in such a way that it can never be recovered. Now at first this seems like a contradiction, on the one hand writing about data security and on the other discussing the ultimate and complete destruction of data. Secure data erasure is an essential task in the context of data security. The following example will explain why it is important to permanently delete data in certain situations.

Let's first assume that the IT infrastructure of a company or organization is to be renewed. What then happens to the old computers, servers and storage systems that will soon be retired? Some companies sell used computers to their employees after deleting data that resides on the systems.

Computers with an operating system still installed are often sold to employees. In most cases, this should pose a problem in terms of licensing. That's why sometimes hard drive n are formatted before they are sold with or without a computer. But there are many free software programs on the Internet that can be used to recover deleted data or to reconstruct data from hard disks that have been formatted before. It is now even possible to recover data from defective hard drives. Therefore, it is not enough to delete data from a hard disk or move it to the recycle bin of an operating system.

To explain why deleted data is often not really deleted, it seems useful to take a look at the ways in which some operating systems store data and how the delete function is implemented in such systems. Before we can store data on a disk, it is necessary to first determine how the stored data will be organized on the disk. This selection and the accompanying initialization of a data carrier are called formatting. Common formats are for example FAT32 and NTFS for Windows systems or ext3 when using Linux operating systems.

If you delete a file on a Microsoft Windows operating system and then open the system's recycle bin, you will find the deleted file right there and you can restore it at any time using the context menu (right mouse button). What happened to this file? Obviously, it was not really deleted. Physically, all parts of the file are still in the same place on the disk where they were before the deletion. Only the link to the file has been moved from any directory to the recycle bin. For this reason, sometimes files or even complete directories that have been "deleted" over a period of years can be found in the recycle bin of an operating system.

In the context menu of the recycle bin, a function is available to delete files or directories from the recycle bin. This function is called "Empty recycle bin". Actually, one would assume that with emptying the recycle bin a file would be irretrievably lost or deleted. However, this is far from being the case even after using this function. You can still assume that all parts of a file are still physically present on the hard disk. Only the storage space that was reserved for a corresponding file is released when it was displayed in the recycle bin and the recycle bin is emptied. In times when hard disk capacities were still specified in megabytes, freed disk space was often reallocated quite quickly. Nowadays, disk space is no longer as scarce and valuable as it was in previous decades. For data carriers with a capacity of several terabytes, it can take years, depending on the use of a computer, until released memory segments are overwritten and thus a part of a deleted file or a complete file is no longer present on the storage device. As long as supposedly deleted files have not been overwritten, it is possible to recover them. For this purpose, there are numerous programs, some of them free of charge, that can search

data media, display recoverable data and recover files that a user already deleted years ago using the means of the operating system.

Hackers and criminal subjects are known to buy old computer systems or hard disks at flea markets or on the Internet and try to recover data on these systems. Even formatting operations that warn that all data will be lost if executed can be undone using appropriate software, at least as far as the storage devices used are magnetic media. During such recoveries, it is not impossible for criminals to get their hands on credit card numbers and other useful data and information.

Recovery software is extremely useful when disks have been damaged or data has been accidentally deleted. However, as we have seen here, such systems can also be used for criminal activities.

For this reason, it is necessary to delete data irretrievably. Secure deletion can be defined in such a way that the deletion procedure means that the data concerned can no longer be recovered with a reasonable amount of effort. The justifiable effort depends, of course, on the explosive nature of the deleted data. If, for example, it is state secrets that were stored on a computer or server, the hard disk should definitely be shredded.

Software tools that are specially designed for secure deletion of data can be downloaded from the Internet just like programs for data recovery, some of them free of charge. Useful systems not only delete a file or directory, but overwrite the data blocks up to 36 times, so that it is rather unlikely to be able to reconstruct the data deleted in this way. To be able to speak of a secure solution, data should be overwritten at least seven times. Some erasure tools are capable of securely erasing complete hard disks.

If a hard disk is to be completely destroyed, it is recommended, as already mentioned above, to disassemble the device completely into small pieces. Usually, special shredders are used for this purpose.

Heat exposure or strong magnetic fields are often not suitable methods for completely destroying data on conventional magnetic data carriers, unless the heat exposure causes the data carrier to melt. With regard to the destruction of hard disks, there are many different methods, some of them very creative but also abstruse. One such curiosity can be seen in Fig. 10.1. The two metal disks are the magnetic data storage devices from inside a conventional hard disk. While the “Texan” method of data erasure shown here may be potentially amusing, it does not securely erase the entire hard drive’s data. With special computer forensics equipment, data could still be reconstructed even from this severely damaged medium. Therefore, one should not try to develop one’s own procedures of data medium destruction and have the data medium destroyed by certified specialized companies. Mind you, a hard disk is



Fig. 10.1 Calibre .44 Magnum and other creative ideas are not suitable as a secure method of data destruction

usually destroyed if particularly sensitive data was stored on it. Such a data carrier is not suitable for conducting experiments.

File systems of other operating systems not considered in detail here use other methods to organize and delete data. However, tools for secure deletion are available for almost all operating systems.

The most effective way to destroy hard drives is, of course, to shred them. The operating system then no longer plays a role.

Currently, more and more computer systems are equipped with memory chip-based data carriers (SSD¹). This type of data carrier has no moving parts like conventional hard disks. Their mode of operation is similar to that of a USB stick. In most cases, if a system failure occurs on such a disk, it is not possible to recover the data because many manufacturers do not publish the algorithms used to manage the data on such disks. It is true that there are some descriptions in the literature of how easy it would be to securely erase data from SSD devices. However, since most storage algorithms are not publicly available and thus basic knowledge about the internal structure of many of these storage devices is lacking, a blanket statement about the degree of security of deletion in this regard seems misguided. Insofar as confidential data was stored on such a data carrier, it therefore appears to be the undoubtedly safest variant of erasure to shred SSD devices in general.

¹ Solid State Disk.

A practical example will show in the following that decommissioned computers or servers are sometimes simply forgotten, even though sensitive data is still stored on them.

In the course of an act of sabotage perpetrated by a former software developer of the company concerned, developments from a period of more than two years were deleted. The saboteur had not only deleted the server directory of the company's most important project, but also manipulated the data backups. Initially, this seemed to mean that the project data was lost. Since this circumstance posed a threat to the company's existence, an information technology expert was consulted promptly. During the initial consultation, the expert already recognized that the server, whose directories had been partially deleted, was the latest model from a well-known manufacturer. The model found had only been available on the market for a short time. For this reason, it was first questioned when the migration of the server to the new hardware had taken place. According to the company management, this process had taken place less than four weeks ago at the time of the interview. The next question asked whether the old server had been deleted and disposed of. At first there was no answer to this question. At this point, no one present could say what had been done with the server that had been discarded. After a short search, the device was then found in an open basement room of the building. All data transferred to the new server during the migration were still stored on the device and it was possible to reconstruct the most recent version of the development project with the help of some records.

Even if the particular circumstances of this case allowed for a good ending for the company, it is absolutely unacceptable that a system with the most important business secrets and developments of a company is disposed of in an open basement of a building used by several companies or forgotten in a dark corner. It was a rather fortunate coincidence that the device was not stolen.

Another source of danger is also often underestimated in the course of data destruction. It is not enough to take care of the deletion of electronic data. It can be equally risky if a company does not take care of secure paper shredding. Documents from offices, ministries, organizations or law firms can cause serious problems if they fall into the wrong hands. Therefore, paper documents should also be sufficiently securely shredded when they are no longer needed. Preferably, shredding of paper pages should be pursued horizontally and vertically, with the smallest possible snippets being desirable. In the case of shredding highly confidential data, it makes sense to burn the shredded paper.

- ▶ **Note 23** *Use only secure methods for deleting data.*
- ▶ **Note 24** *Don't forget trade secrets or sensitive data on segregated devices.*



Data Backup and Restore

11

Abstract

The user usually only realizes how important a data backup is when it is necessary to use the corresponding backup to restore a system. Sometimes it is not necessary to use a data backup in a company for years. This can also lead to carelessness in the use of data backups. However, if a disaster occurs, a well thought-out and conscientiously executed data backup can, under certain circumstances, ensure the continued existence of a company. The chapter shows common mistakes in connection with data backup and explains some procedures that can significantly reduce the consequences of damage events.

First of all, it should be emphasized here that importing a backup is the last resort of all measures when a system or database has been destroyed and can no longer be made available in any other way.

In some cases, data backups are also used for other purposes. This can also be a way to defraud the tax office. One such case is known from a doctor who regularly wrote several invoices with the same invoice number. It can be assumed that only one receipt per invoice number was reported to the tax office. In order to carry out this fraud, the doctor made a backup copy of a database before creating an invoice in the software belonging to the database. After creating and printing the invoice, he immediately restored the backup and had the same invoice number available again.

Backups are not intended for such excesses. The reader is strongly advised not to try something like this himself or even to support other people doing it.

As we have seen in the previous chapters, a backup can be invaluable to any organization when a hacker attack has occurred, a virus has entered the system, data has been encrypted, or when systems have been destroyed by water, fire, or other

impact. In such situations, a backup is often actually the last chance to restore a system. Therefore, it is necessary to plan backups comprehensively and to check regularly whether a restore is possible. The way in which backups are planned depends on the importance of the system being backed up and the amount of data being stored and processed there.

Even though there are significantly more variants of data backups, in this chapter we will only look at the most commonly used types: The incremental and the full backup.¹ As the name implies, the full backup includes the total amount of data of a given system or even the entire executable system.

In the event of a disaster, the full backup is also the most preferred type of backup. Incremental backup only saves changes that have occurred since the previous version of the backup. When a system is to be restored using incremental backup, it is always necessary that the last full backup is also available. Therefore, it is usually more complex to restore a system using incremental backups. Now, of course, the question arises as to why this type of backup is used at all. Sometimes it is necessary to perform more than one backup per day. For some online services that are available all over the world, so much data can be generated that a backup is necessary and performed every five to ten minutes. In such a case, it would not be efficient to run a full backup every few minutes, as this type of backup could potentially take several hours. In such a case, it makes sense to create a full backup once a day and perform incremental backup s every few minutes.

In many cases, it is not sufficient to just make a backup of the data. For example, let's say that an ERP system is damaged by a water leak and you had previously made an up-to-date backup of that system's database. To restore the system, you need new hardware or a virtual server, an operating system, the database management system (DBMS) used by the ERP system, and the correct version of the ERP software to restore the database data. At this point, it becomes clear that having a database backup is not enough in an emergency when the complete system needs to be restored very quickly. In such a case it can be of great advantage not only to rely on a data backup, but also to keep an image backup of the computer. Such an image² can be stored as a so-called bare-metal recovery backup. This means that in the event of a server disaster, a system can be restored on different hardware or even as a virtual server. Such a backup does not necessarily have to be created every day. If the data is backed up separately, it is sufficient to perform an image backup if

¹Garfinkel/Spafford, *Practical Unix & Internet Security*, 2nd ed. O'Reilly & Associates Inc., 1996.

²System image.

significant changes have been made to the operating system or the ERP system used.

With a combination of image backup and backup of the processed data or the database, a system can be restored in a manageable period of time. These procedures are also suitable for smaller infrastructures and stand-alone computers that require a high degree of availability.

- **Note 25** *Make sure that not only data but a complete system can be recovered.*

What can happen when a system is restored?

As mentioned at the beginning of this chapter, restoring a system by means of a data backup should be the last resort of all measures.

Therefore, let's consider what will happen if you need a backup and it turns out to be non-functional because it has been corrupted in some way. There is a known case where the employees of an organization had changed the backup media (tapes) every day and the backup software used marked each backup "OK". The backups were never tested and when a backup was needed after a few years, it was discovered that the backup tapes no longer had any coating at all, which would have been required to store any data at all. There was no functioning backup within the organization at that time.

- **Note 26** *Test the data backups regularly.*

To save yourself from such an experience, it is recommended to check backups regularly. The most practical way to do this is to perform a restore test in a special test directory.

Never test a restore by overwriting the data of the backed up original directory with the restore. The importance of testing backup and restore is illustrated by an example where a virtualized server was destroyed on the first attempt to create a backup.³

There are a few methods that can be used to ensure that backups are available when needed. A storage device connected by a UNC⁴ path (for example, NAS) must

³Greguš, M; Lenhard, Th.; Case Study - Virtualisation of Servers in the Area of Healthcare-IT; published in International Journal for Applied Management Science & Global Developments, Bibloscient Publishing Services, Birmingham, 2012.

⁴Uniform Naming Convention.

never be the only place where backups are stored, as some current viruses have the nasty property of encrypting all drives and hard disks connected to an infected system. Therefore, offline backup s, stored in a safe deposit box, for example, may be necessary for an organization to survive a virus attack economically. In the event of a fire, it is also useful to keep an offline backup outside the office.

Since backups usually contain confidential data, in case of off-site storage it is recommended to secure them with a password and to store them encrypted or on an encrypted device.⁵

► **Note 27** *Keep encrypted backups safe outside of the office.*

⁵See Garfinkel/Spafford, *Practical Unix & Internet Security*, 2nd ed. O'Reilly & Associates Inc., 1996.



Abstract

Since ancient times, encryption has been a tried and tested means of ensuring that no unauthorised third parties can read a message during transmission. This is no different in the age of e-mail and the Internet. Those who think that it is not possible to analyze billions of e-mails every day may be inclined to place more trust in this means of communication than it deserve. This chapter explains what types of encryption are available to us today, what we should use encryption for, where encryption is used in the world of information technology, and what encryption algorithms we should never use.

If you work with encryption, please keep in mind that the use of such methods is not legal everywhere in the world.

What can we use encryption—also called cryptography—for?

Since ancient times, methods of encryption have been used so that no unauthorized third party could read a transmitted message on its way between sender and receiver. Both the sender and the recipient had to possess the key that was used to encrypt and decrypt the message. When the same key is used for both sender and receiver in this classical type of encryption, it is called symmetric encryption.¹ The way a message is encrypted or decrypted using the key is called an algorithm.

The strength of the encryption depends on the algorithm used as well as the key length and its complexity.

¹Schneier, Applied Cryptography, Addison-Wesley, 1996.

Today, encryption methods are used for files, directories, storage devices, data containers, backups and for secured communication channels such as VPN² or HTTPS. Besides symmetric encryption, we also know methods of asymmetric encryption and encryption using trapdoor algorithms. Trapdoor algorithms can encrypt something, but are not able to reverse the encryption.

Such algorithms can be used for login procedures. In this case, a system contains information about user accounts and an encrypted password for each user. When the user starts a login procedure, he uses his account and his real password. The password is encrypted by the trapdoor algorithm and compared with the stored encrypted password. If both encrypted passwords match, the login procedure is completed successfully.

However, it should not go unmentioned that such procedures have caused numerous problems, especially with older UNIX and Linux distributions. Until the turn of the millennium, some systems stored the encrypted password in a file found in a special directory called “/etc”. In the 1990s, it was therefore relatively easy to break into UNIX and Linux systems that were connected to the Internet. Connected to a server via FTP as guest or user “anonymous”, it was possible to download the file “passwd” from the directory “/etc”. This file contained the user names in plain text and the associated passwords in encrypted form. At this point, most hackers were not able to break the encryption used. However, this was not necessary. At that time, it was already possible to download text files from the Internet that contained complete dictionaries in every conceivable language. A small program was able to encrypt each word of such a dictionary with the same trapdoor algorithm that was used by operating systems and match it with the keys stored in the file “passwd”. In addition to the standard dictionaries, one could also use self-defined dictionaries in which frequently used terms were combined with numbers and special characters, such as “test*” or “test123”. The latter is said to be one of the most popular passwords worldwide even today.

In the 1990s, this simple method made it possible to hack into offices, ministries, military systems, organizations and companies connected to the Internet.

Even though UNIX and Linux systems now store encrypted passwords in a different, specially secured file, and most organizations use professional firewalls to protect their systems from the dangers of the Internet, this early version of a so-called brute force attack is still in use—in modified versions.

For this reason, passwords should never be found in a dictionary and should have a minimum complexity. Some sources recommend using passwords with a

²Virtual Private Network.

minimum length of eight characters. However, since the password is nothing more than a cryptographic key, using a minimum length of twelve characters, combining lower and upper case letters with numbers and special characters, is a significant improvement in security.

A secure password could therefore look like this: **R&b!Im0Z2#Vy**

► **Note 28** *Use only complex passwords.*

To defend a system against such brute force attacks, it is recommended to lock or disable user accounts if multiple incorrect passwords have been entered for them. In wireless networks (WLAN³), it is also recommended to block user accounts or MAC addresses when a predefined number of unsuccessful connection attempts have occurred (for example, after three, five or ten unsuccessful authentication attempts).

► **Note 29** *For all login procedures, the number of possible failed connection attempts should be limited.*

Now let's look at another type of encryption. Asymmetric encryption uses one key to encrypt data and another key to decrypt data or messages. A distinction is made between a public key and a private key.

A major advantage of asymmetric encryption over the symmetric method is that a public key does not have to be exchanged under great security precautions.

A public key can be made available or downloaded anywhere on the Internet, since once encrypted data can only be made readable by the private key.

Therefore, the private key must be protected as well as possible.

One of the most widely used systems that works with public and private keys is PGP⁴. For secure e-mail communication it is necessary that both communication partners have the public key of the other.

How secure are encryption systems?

The state of the art is constantly evolving. That is why it would be quite conceivable that a method that is described as safe at the moment of writing this book is outdated when this book is available in printed form a few weeks later.

One thing is clear: In the meantime, there are some methods of encryption that are considered insecure and outdated.

³Wireless Local Area Network.

⁴Pretty Good Privacy.

Above all, the original DES⁵ algorithm should not be used under any circumstances, because contrary to what its name implies, it has already been considered insecure for years. In the area of wireless networks, there are also various encryption systems whose use should be avoided at all costs. The encryption methods WEP⁶ and WPA⁷ can be overcome in a few minutes even by laymen with instructions from the Internet.

When thinking about encryption methods, it is always necessary to inform oneself about the state of the art.

To conclude this chapter, a brief explanation of end-to-end encryption is provided. When you send an e-mail and establish a connection with SSL /TLS to your provider, you know that a secure connection is established between your computer and the provider's outgoing mail server. However, you have no influence on what happens to your e-mail between the outgoing mail server and the recipient. If several providers are involved in the transmission, we cannot even determine the exact path an e-mail takes through the Internet. On this path, which is figuratively in the dark for us in most cases, a lot can happen to our e-mail. For example, it can be analyzed for specific keywords. To perform such an analysis, there is no need for a person to read the email; rather, analytics programs are now capable of analyzing billions of emails daily, combing them for keywords and categorizing them accordingly. In 2014, a test was conducted among some experts to see how effectively such systems work. For this purpose, a German engineer sent a fake email to a recipient who was informed about the project. In this mail, the engineer reported on the development of a jet engine that was supposed to work thirty percent more efficiently than conventional engines. Funnily enough, the subject had never dealt with the technology of jet engines before, but three weeks after the mail found its way through the Internet, he received an offer of employment with an aerospace company outside Europe.

Even IT experts today can hardly say which encryption methods are really secure. For this reason, we should always be careful about what we send encrypted or unencrypted by e-mail.

In plain text, we should anyway only send information that we could also easily send on the back of a postcard. But even if we critically question the security of cryptographic processes, there is no doubt that they can protect us from many criminal activities on the Internet.

⁵Data Encryption Standard.

⁶Wired Equivalent Privacy.

⁷Wi-Fi Protected Access.



Abstract

Using examples, the chapter explains how easy it can be to trick websites that are based on so-called content management systems and to log on to such systems as an administrator. Although the security vulnerabilities used here are usually due to negligence in development or administration, the methods described are still common.

In the meantime, there are probably thousands of methods to attack websites or web-based services and databases. Two of the simplest, but still very successful methods are described here. Please use this information only for legal purposes.

The first method is based on the fact that to this day many web developers or administrators of web portals are not serious enough about the security of the systems they develop or maintain. Especially when they have to work with multiple systems, they often use the same passwords for all systems or use default passwords predefined by a software vendor. There are many systems on the internet that only use the default password for an administrator account. These could be CRM¹ systems, shops, online services or even normal websites that use a content management system. If you are looking for such a content management system, all you need to know is the name of the file that is required to log in. Let's say the name of the file would be "adminlogin.php". Then you can use a search engine that allows you to search in URL paths, such as Google or Bing. If you use "inurl:/adminlogin.php" as the search term, you will get numerous hits. Some of the systems found this way might use the factory default password of the CMS.

¹Customer Relation Management.

- **Note 30** *Never use a factory default password for a system that is connected to the Internet.*

The second example of breaking into a website is also quite simple.

This example is based on the fact that tons of badly programmed systems are used in companies and on the Internet. If the login of a website uses the SQL² language—which is a standardized query language for database systems—to perform a check of user account and password, this login process can possibly be outsmarted unless special security measures have been set up.

Therefore, let's consider a poorly programmed login procedure that uses an embedded SQL statement that can write values to a system variable named "iLoginSuccessful".

The default value of this variable is 0. If this variable is set to 1, access to the web page and to the online database behind it is enabled. The input of the password in a data field is inserted into an SQL statement and compared with the user password in the system database. The SQL statement could then, after addition of user name and entered password, look partly like this:

```
... user.username = administrator AND user.password = "R & b! Im0Z2 # Vy"
```

As far as the user name in the database table is Administrator and the password of this user actually corresponds to the input "R & b! Im0Z2 # Vy", the value 1 would be written to the variable iLoginSuccessful and access to the system would be granted due to the successfully executed login procedure. The default value of the variable iLoginSuccessful is 0, so as far as an incorrect entry is made, no access to the system is granted in principle.

Actually, we don't need the password at all, because we can change the whole logic of the SQL statement via the input field for the password. Instead of the password—let's assume now that we don't know it—we can write some additions into the data field reserved for the password. For example, if we put "hello or 1 = 1" in some special formatting, it will check if the administrator's password is "hello" or if the alternative (or) of this condition 1 = 1 is true. The latter is always true, so the value of iLoginSuccessful is set to 1 and access to the system is granted even though we don't know the password. The main challenge of this procedure is to find the correct syntax for assembling the SQL statement. Several quotes and spaces are needed here.

²Structured Query Language.

This procedure is a common method of logging into poorly programmed and secured systems on the Internet. Currently, there are still many systems that use insecure login procedures. This type of breaking into a system is called SQL injection. Such an intrusion can be prevented if the content of the password field is encrypted and compared with a stored and secure encrypted password.

- **Note 31** *Never use systems with insecure logon procedures, especially when connected to the Internet.*



Common Security Problems

14

Abstract

If an audit is carried out in a company, it almost always reveals procedures that could be summarised under the term routine and about which no one in the company had previously given any thought. These are often small things that could be easily remedied or avoided if only a user were made aware of them. In some cases, however, a lack of knowledge about technology and how devices work can lead to sensitive data leaving the company unnoticed or to points of attack for hackers, even though the latest innovations in information technology are being used in the company. The chapter highlights some security problems that are frequently encountered in companies.

14.1 Working Consoles that Are Not Locked

Sometimes we leave our office or workplace for a short period. For this reason, screen savers are available in popular operating systems. But the screen saver offers little protection against illegal activity unless it is secured by a password. In one case, a CIO of a large data center left his office for a total of fewer than five minutes. Access to the data center was monitored and the rooms were secured with special doors and locks. However, a trainee in the office took advantage of this short time to download and infiltrate a Trojan horse into the CIO's computer from the Internet.

- **Note 32** *Always lock your computer's console when you leave the office or workplace.*

-
- **Note 33** *Activate the password protection in the screen saver of your computer if it cannot be ruled out that other persons gain physical access to the system.*

14.2 Printer Stations and Multifunction Devices

Most users would not expect large printer stations or multifunction devices to have their own hard disks. Such devices often use internal hard disks for the temporary storage of print jobs until they have been processed. But as explained in Chap. 10, modern hard disks rarely forget what was once stored.

Especially when leases for such equipment expire, such equipment is returned to leasing providers, often with all documents that have been printed for years still available or recoverable on the internal hard drive. It is necessary that such hard drives are erased by a secure method or that the hard drives are replaced before such equipment leaves a company or organization.

- **Note 34** *Note that sometimes the print jobs of several years may be stored on internal hard disks in printer stations or multifunction devices. This is especially important when devices are returned to a leasing company.*

14.3 Working with Administrator Privileges

The system administrators account is for one purpose only:

Managing the system!

However, it is a very common practice to declare one's user account to be the administrator. This makes it possible to install software and make setting changes to a system at any time. In many cases, however, this approach is recognized far too late as a serious error. Many Trojans or viruses can only really cause major damage or take root in systems if they are active under a user account that has extended rights. The worst case scenario in this area is an administrator who only uses the domain administrator's account and "catches" a computer virus under this account with maximum rights.

- **Note 35** *The administrative rights are only intended to administer systems. They should in no case be used for daily work on the PC.*

14.4 The Internet of Things and Industrial Control Systems

In the previous chapters, we dealt with computer networks, workstations, servers, printers and other classic components in the field of computer systems. Nowadays, everyday devices are also increasingly connected to the Internet and this causes more and more problems because hardly anyone thinks about the fact that it might also be necessary to protect their refrigerator with a firewall. While computer systems are regularly updated, it is rather the exception that security updates are available or installed for televisions or refrigerators.

If such a device is infected by a Trojan or bot virus, it is almost impossible to fight the malware. Currently, we have to assume that thousands of such devices are infected with viruses worldwide and that many of them are used for illegal activities as part of a botnet. Even if this thought will initially add to the amusement, in the event of an investigation against such an illegal network the question actually arises whether the public prosecutor will secure your refrigerator. In fact, we should assume that most household appliances are not yet secure enough to withstand threats from the Internet. A similar problem can be found in the industrial sector. Some fellow people now think they have found the philosophers stone when they can control all sorts of equipment via a web browser or via a so-called smartphones app. It is best to answer the question for yourself: Is it necessary to control and adjust the parameters of a nuclear power plant via the Internet?

If you answer this question for yourself, you will probably discover that you also believe that today's technology is not sufficiently secure to connect control systems of critical infrastructures to the Internet. Many things that are presented to us today as technological advances are nothing more than "nice-to-have technology". In other words, when viewed objectively, a large number of web-based "solutions" or smartphone apps belong to the "things the world doesn't need" category. Some apps are programmed not because they are desperately needed, but because they can be implemented—however they are implemented. However, security considerations are often left out of the equation.

- **Note 36** *Do not use nice-to-have technology. Especially in very complex or critical infrastructures, it is often best to plan and operate communication*

systems according to conservative approaches. Too much innovation in the area of IT can threaten the existence of a company.

- **Note 37** *Before implementing new technologies, evaluate systems thoroughly and analyze them, especially concerning security issues.*

If production plants or other industrial facilities have to be connected to the Internet for automatic monitoring and, in the event of technical faults, reporting to a manufacturer or service company, the implementation of such a connection must be planned from the point of view of the system security.

This means that such a connection does not necessarily have to communicate via a company's central computer network. Rather, it should communicate with the manufacturer or service company via a separate network segment that is separated from the company's other network by a professional firewall system. The same recommendation also applies to so-called pioneer buyers who purchase the latest devices in the private sector that are connected to the Internet. A firewall can also prevent your refrigerator from acting as a node of a botnet.

- **Note 38** *A firewall that is suitable for professional purposes can reduce the dangers of new technologies.*



Identification of Computers and IP Addresses

15

Abstract

Regardless of whether an attack on IT systems comes from the internet or from within the company, it is necessary to identify an attacker to prevent further attacks or to hold the attacker accountable. The same applies, of course, to other forms of computer crime. The chapter shows how specific computers can be found, how the connections used by criminals can be identified, and how the personal details of a criminal can theoretically be determined via an entry in a router.

In some cases, especially in the fight against cybercrime, it may be useful or necessary to identify a specific computer or the IP address of an internet connection. Many possibilities can be used for this purpose.

In the following, two cases are described in which very simple methods were used to identify criminals or to identify their internet connections.

In the first case, a criminal tried to sell an expensive measuring instrument at a low price on the internet. Allegedly, the seller lived in Edinburgh/Scotland. When contacted by a potential buyer, he looked for excuses why the device could not be picked up at his given address in Scotland. He suggested instead that the device be sent by post after it had been paid for through the service of a supposed escrow company. The website for this “escrow company” turned out to be a complete fake. The bank account to which the money was to be transferred was held at a Polish bank, although the alleged company was supposed to be based in Germany. First, the fake website was identified. To do this, the command line program Ping was used, which is available in most operating systems. To find out the IP address, it was

only necessary to enter the following command in the command line and press Enter:

Ping <Web Address>

The program immediately returned the IP address of the corresponding page. To be able to assign the IP address to a location or a company, there are several free services on the internet. In the case described, this website was located in a data center in Germany.

The next step was to identify the imposter.

Free service on the internet was also used for this. You can have a link generated on certain servers on the internet, which you can send by e-mail. When you generate the link, you simultaneously register your e-mail address as the service's reply target. As soon as the sent link is clicked, you receive an e-mail with the IP address of the recipient of this e-mail. In addition to the IP address, the e-mail also contains an exact timestamp. The latter is necessary because many internet users receive a dynamic IP address for each session on the internet through their provider. In this particular case, it took several emails with this link and a nice story to get the criminal to click on the link. The next morning, the local police rang his front doorbell.

Even though this is a very simple example, it should show that it is possible to identify every computer on the internet because every criminal needs a node or a provider to gain access to the internet.

Now, you may be wondering how we can identify a criminal when he is connected to the internet through the illegal use of wifi.

This is now explained in the second, also quite a simple example.

In this case, a criminal sent death threats by e-mail. The internet connection was quickly identified and it was just as quickly determined that the criminal had connected to the internet via a company's WLAN. When you connect to a WLAN, this device stores the connection data, sometimes even without a time limit. Therefore, in some WLAN routers, you will find the names of all computers that have ever been connected to the Internet via this component. The IP address is not of interest to us in this case, because most WLAN routers work with DHCP.¹ This means that connected computers receive a dynamic IP address from the router. But one thing is almost always available: The MAC address (see Chap. 3) of the connected computers.

¹Dynamic Host Configuration Protocol.

A MAC address can be faked, of course. But if someone has connected his computer to the real MAC address, there is a real chance to identify the computer. Through the MAC address, you can identify the computer manufacturer. Most modern industrial companies work according to ISO²9001. This international standard for quality management and documentation ensures, for example, that after the manufacture of a production batch in which defective components have been installed, all finished products can be identified as defective, because each product has its history and is assigned to the corresponding batch.

This means nothing more than that the computer manufacturer can identify any computer built by that company by its MAC address. But that's not all: some manufacturers work with direct sales. Other manufacturers offer their customers an extended warranty or special services if the buyer registers his computer. In these cases, manufacturers have personal information, including the address or at least the name, phone number, and email of the customer who purchased a particular piece of equipment. To the extent that registration of a computer is not available and the computer was not purchased directly from the manufacturer, it is still possible to trace to which dealer a manufacturer or wholesaler sold a device. As far as the device was not paid for in cash at the dealer, but was purchased by EC card or credit card, the seller can also be identified via the distribution chain. If all these ways do not lead to the desired result, it is still possible for a MAC address to be identified by internet providers. Depending on the national legal situation, this may be easier or more difficult. From a technical point of view, it is possible in any case.

²International Organization for Standardization.



Abstract

Firewalls have long been part of the standard equipment of companies. But not all firewalls are the same. This chapter explains what to look for when selecting a firewall system and what to consider during configuration.

When we are faced with a large fire with flames 30 meters high, it is understandable that this wall of fire is difficult for us to overcome. However, if the flames are no higher than a few centimeters above the ground and the fire does not have a large surface area, we would simply jump over it or walk around it. This comparison describes quite well the situation when using technical firewalls in the world of computer science. Some firewalls are very effective, while others just pretend to be secure. However, since the dangers from the internet are real and are constantly increasing in intensity, quantity and danger potential, the impenetrable large fire should be used, to use the figurative comparison once again. In this context, this publication often refers to a professional firewall. But what are the differences between firewalls for professional use and—let's just call them toy firewalls?

A firewall separates different networks. Normally, these networks have different IP number ranges. A distinction is made between private and public IP numbers. A private IP number, as used in a small network, for example, would be:

192.168.2.10

These private IP numbers are not forwarded on the internet.

But coming back to the firewall, such a device (it is also available as a software solution) should not only separate different networks but in an intelligent way

control and monitor the communication between the networks. Therefore, it is also fundamentally necessary for a firewall to know what communication is allowed and what connection attempts it should prevent. Some inexpensive firewalls only check the IP numbers involved when a connection is to be established.

Let's assume that in our company or organization, we would run a server that uses the IP address 131.58.40.100. In the same network, let's further assume, there are client computers with other IP numbers of this IP number range. Now a communication request reaches the firewall. A device with the IP number 131.58.40.17 tries to connect to the server and establish communication. At first glance, this seems to be OK and a simple firewall would forward the data packets without further investigation. However, if the source of this IP address is on a different network or even originates from the internet and it is a spoofed IP address, the hack of our firewall and server is almost complete. It is therefore of elementary importance that a firewall identifies the network from which a packet originates. If a packet originates from a network that does not match the specified IP address, access and transmission must be denied immediately. In addition, modern firewalls also remember which computer from the internal network has made a request to a server on the internet and only allow responses from the internet if they can also be assigned such a request. Such firewalls with advanced analysis functions are called stateful inspection firewalls or simply intelligent firewalls.

Hardware firewalls are often extended with so-called proxy functionality. Such devices are not only able to filter data traffic and reject unauthorized connection requests, they can even block websites with dangerous or radical content. In addition, such firewalls are also able to scan data traffic for viruses and malware and block connections from infected computers to malware servers on the internet.

Appropriate devices (see above) should be part of the standard equipment of every organization and every company whose IT systems have access to the internet.

► **Note 39** *Firewalls should always be state of the art.*

Usually, in most cases, a firewall is not completely opened for a special IP address or a MAC address. Instead, special ports are required for a planned communication (see Chap. 3). Therefore, only those ports should be opened in the firewall that is required for a planned communication.

To find out which ports are open in a firewall, a so-called port scanner can be used. This is a software program that tests the possibility of connection for all ports one after the other. Such port scanners are available for free on the internet and can sometimes provide valuable assistance in identifying configuration problems. A

large healthcare organization commissioned a test with a port scanner from the internet some time ago. In less than a minute, the tester found an open port and a few seconds later saw the domain controller login dialog on the screen in front of him. The corresponding security hole was closed immediately.

- **Note 40** *Ask an expert to hack into your system to improve data security. But do not give him any passwords for this purpose.*



Abstract

Without a router, there is no connection between a local network and the Internet. So whatever data is exchanged with servers on the Internet must inevitably pass through the router. Successful attacks on corporate networks are also likely to occur via the router in many cases. Therefore, this chapter deals with the function and importance of the router for communication inside and outside a corporate network and provides suggestions on what to look for when using appropriate devices.

In some of the previous chapters, we talked about WLAN routers or firewalls. Nowadays, the technical boundaries between the different devices are more and more blurred, because hardware firewalls can have the functions of routers integrated and routers often have the functions of firewalls integrated. However, if we want to communicate with the Internet from our organization's network, we cannot do it without routing and without the functionality of a router. Routers work on the third OSI¹ layer. We remember: this layer takes care of the correct routing between the sender and receiver of data packets. Routers connect networks or network segments that use different address ranges.² For example, if a network in an organization uses the IP address range 192.168.2.x (private network) and the organization uses a fixed IP for Internet communication, for example, 79.246.238.175 (public address), then the router knows that data packets intended for communication with an Internet service must be forwarded to the Internet

¹Open Systems Interconnection (see also Chap. 3).

²Dausch, Netzwerke - Grundlagen, Herdt-Verlag, 2014.

accordingly. The latter is represented internally in the router by the fixed IP address shown above.

Since routers are also used within organizations and companies to realize the communication between individual network segments, the so-called routing table is an essential feature of such devices. This means that the router knows in which network or in which network segment a certain network address can be found.

Most common operating systems allow the definition of a standard gateway.

Even though the term gateway stands for a device whose switching activity is not limited to the third layer of the OSI model and therefore also supports communication between networks with different network protocols, the so-called standard gateway of most networks is a router. Since the routing functionality, which works through routing tables, can be easily outsmarted, it is recommended that a router is never connected to the Internet without a suitably professional firewall. The use of a firewall or firewall router can also be useful within an organization or company, even if only internal network segments communicate through it. Using an incident in a medium-sized company as an example, we will explain why this is the case:

A system update, which a service company had transferred via VPN³ to the server of the personnel department of an organisation, was infected with a virus (sic!). After installing the update, the computers of the entire department were infected. However, since all segments of the organization's network were separated by firewalls, the virus was unable to overcome the firewall and spread throughout the organization. The overall damage caused by this incident was manageable.

But firewalls can also be extremely useful when members of an organization or employees of a company trying to spy on information—for whatever reason—that they don't need to do their jobs.

- **Note 41** *Never connect a router to the Internet if it does not have a professional firewall or an additional firewall.*
- **Note 42** *In larger organizations and companies, it makes sense to also separate network segments (departmental networks) from each other using firewalls.*

³Virtual Private Network.



Abstract

The usability of an antivirus system or other security software is a fundamental success factor for achieving desired protection goals. This chapter shows common pitfalls in the use of security systems, gives an overview of how antivirus and security systems should be selected and how the protection of infrastructure can be improved by combining several security systems.

As far as computers or computer networks are connected to the internet, it is one of the most fundamental technical and organizational measures that the computer is also secured against dangers from the internet. The higher the security requirements, the more complex is often the corresponding systems. Although Chap. 16 recommends using only devices that are suitable for professional use, simply purchasing such a device does not necessarily mean that a network is adequately protected. The same applies to antivirus and other security software.

An example from the area of public administration may illustrate this. After an administration wanted to put a web-based citizen portal into operation, there were difficulties in this regard to reach different services of the web server from the internet. Apart from the fact that a web server should usually be located in a DMZ network and not directly in the main network of a company or an administration, it is common for different ports to be used for certain services offered (see Chap. 3). After tests showed that not all services could be used from the internet, the IT manager “labored around” on the firewall until the portal could be accessed without problems. This success was only of very short duration because the IT manager had defined “ANY-ANY” as the access rule with the highest priority. In the context of the firewall used, this meant that all incoming and outgoing data traffic was allowed.

Since this rule was applied with the highest priority, all data traffic passed through the firewall unfiltered. The setting corresponding to a constellation in which there would be no firewall at all. The situation was also made more dramatic by the fact that some of the operating systems used in the administration network had already been discontinued by the manufacturer years ago (see Chap. 6). After a very short time, the servers with outdated operating systems were already infected by various malware, which spread from there both internally and externally. Although security software was installed in the network, which can combat viruses and malware, this was configured with just as much care as the administration's firewall. Viruses were detected and reported, but they were not deleted or otherwise removed. Users were therefore regularly informed about the contamination of their computers, but the threat was not combated. Only the help of an external team brought an improvement to the situation. After cleaning up the network and shutting down computers with outdated operating systems, the firewall was programmed in such a way that only those ports allowed data traffic that were necessary for the operation of the corresponding systems. In addition, servers accessible from the internet were taken out of the main network and integrated into a DMZ¹ network. The amount of virus and malware contamination was enormous at this point. Each computer was individually cleaned of viruses and to prevent further spread of viruses and malware, the program execution control of the protection software was activated. As long as this is active in a domain-based network, only programs whose execution has been explicitly permitted by the administrator can be executed on the monitored computers. Although such a function prevents a virus from spreading again in the network, it should not be underestimated in terms of the administrative effort required. Software that is normally and regularly used in a network must also be approved and sometimes an execution control recognizes different versions of a software as different programs. This means that even in networks with less than 100 computers and servers, a high number of program requests from the security software must be answered.

However, the example shows first of all that a security system may remain ineffective if there is a lack of knowledge within the company or institution on how to configure it correctly in the specific environment. In this case, the internal IT administrator was completely overwhelmed by the complexity of the systems in use.

¹Demilitarized zone = Network that is separated from other networks by a firewall and to which access is possible from there (e.g., from the internet).

- **Note 43** *If resources or know-how for the effective use of security systems are not available within the company, you should have such a system managed by reliable external experts.*

However, the cause of misconfigurations is not always entirely the responsibility of the company that purchased and deployed the security software. In another case, a centrally controlled antivirus solution was to be updated by experienced administrators due to the discontinuation of the older version in a medium-sized company. Until the update was carried out, the system worked reliably. Despite compliance with all requirements, the system update led to significant problems. The distribution of the security software to clients no longer worked, clients were sometimes no longer found by the security software at all or were displayed as not integrated after a short time, although everything seemed to work before. The laborious contacting of the company's technical support did not bring any improvement. The quality of the company's support was comparable to that of numerous forums on the internet where more or less clueless contemporaries regularly give useless advice in fits of hubris. Three times alone, the same files and information were requested, which had been generated by a check tool provided by the respective provider. Then the administrators were told that they would have to create a new task in the support portal for each partial problem. However, none of the problems were solved by the support. It was then recommended to install the latest version, in which the problems were supposedly solved. However, at that time the system was already up to date. Therefore, the administrators reinstalled the entire server. The security software in the latest version showed the same malfunctions, so that only one conclusion was possible, namely that the new version with which the discontinued program version of the provider was to be replaced, was extremely faulty and the support offered was completely inadequate. The administrators then decided to test security software from other providers and not return to the previously used system in the future. Vendor support is often only needed when serious problems with a software or system occur. Then realizing that the sometimes expensively paid support is useless, usually exacerbates the problem that has arisen. In this specific case, however, it also became clear that it makes sense not to rely on test reports from magazines. Insofar as the suppliers of protection systems are advertising customers of certain magazines, the question arises from time to time as to how objective a critique or a test concerning such a product will turn out to be. There are also sometimes striking differences between the assessments of different tests, depending on the magazine or internet forum in which they were published.

- **Note 44** *Do not rely on marketing or advertising claims when selecting security systems.*

Antivirus and protection systems are usually relatively uncritical as long as they are installed on individual computers. However, the installation of such systems in a company network becomes more difficult if settings, software and update distribution are to be handled centrally via a server.

In summary, problems can result from the following main circumstances:

- The software is too complex for the user
- The operation of the software is not self-explanatory
- The software is faulty
- The support for the software is poor or completely inadequate

When selecting the appropriate software, it should therefore first be clarified whether this is to be maintained and supported internally or whether an external service provider is to be used for maintenance and support in this respect. If the system is maintained by an external service provider, this provider will usually specialize in the maintenance of systems from one or two manufacturers. However, a company that has its security software or firewall managed by a service provider is placing itself in a certain dependency. The service provider should be known to be reliable and, in particular, proof should be provided that the employees of the service provider entrusted with the subsequent support of the relevant systems in the company are also regularly trained concerning these systems. Especially if the company does not have the necessary know-how to manage security-relevant systems itself, such systems should be managed by reliable external service providers.

If external service providers are not used and the selection of future security software should be made by the company's employees, a comprehensive test of systems is recommended in any case. Virtualization technology, which has become widespread in the meantime, allows comprehensive tests to be carried out with minimal installation effort.

- **Note 45** *The selection of security software that is to be operated without additional purchased services should therefore always be preceded by a comprehensive evaluation.*

The end-user does not usually have the opportunity to examine the programming code or search algorithms of anti-virus software. If widespread security software is

used, it must therefore be assumed that it will usually fulfill its purpose of identifying and eliminating viruses and malware. Therefore, when selecting such software, the main focus should be on intuitive usability. The software should be easy to install for test operation and work without errors. If problems occur during the test run, it can be assumed that they won't get any less during live operation. Support should also be tested. In particular, the question arises whether telephone support is available that can be reached regularly or whether support cases can only be reported via a cumbersome internet portal with prior login and registration and the inquirer then receives a more or less helpful e-mail at some point.

- **Note 46** *Comprehensive support should be ensured for self-managed security software. This includes, in particular, the possibility of contacting support by telephone at short notice.*

In connection with the selection of antivirus or other security software, the question also arises as to whether it makes sense for a company to rely on the product of only one particular manufacturer or whether it would be better to use several antivirus systems.

This question is relatively easy to answer. If we assume that none of the current antivirus systems can ensure a detection rate of 100% in the long term and that the systems usually have different strengths and weaknesses, then it is obvious that the detection rate within the network can be improved if different antivirus systems are used in a multi-level arrangement. Or to put it another way: If we use the same antivirus software on all computers, then an e-mail may be scanned for viruses using the same scanning routines on the proxy server, the e-mail server and the end device. However, triple scanning with the same software adds no value. Let us now assume that a virus is so new in its coding and has been developed so subtly that a corresponding virus definition, i.e., a corresponding identification possibility, is not known to the anti-virus program used or this is outwitted by a virus, then in the worst-case scenario the virus-infected e-mail would pass through all three instances without the danger being detected. For this reason, you should work with several different anti-virus and protection systems, wherever possible. Of course, this only makes sense where a corresponding IT infrastructure is available.

- **Note 47** *Where a complex IT infrastructure is in place and where it is possible to do so, different anti-virus and protection systems should be used, complementing each other in multi-stage checks.*

As already described, a corresponding configuration could look like this: Servers and end devices in the network are monitored by a centrally controlled protection system. However, if data packets of internet communication or e-mails were routed via proxy servers and filtered there, it would seem to make sense to use different security software there. However, the number of inspection levels and the different protection systems used always depends on the specific structure of an IT infrastructure.

If an e-mail server is used in the company that interacts with e-mail clients on the end devices, it also seems to make sense to install a different antivirus or protection program on the e-mail server than is available on the end devices.

Firewalls, antivirus, and security software are only as good as they are programmed by the developer and configured by the administrator.



The Demilitarized Zone

19

Abstract

An increased risk potential for IT systems and infrastructures always exists when resources within the network can be accessed and reached from the internet. The chapter describes the use of so-called demilitarized zones and the use of proxy servers to better secure corporate networks against attacks from the Internet.

Hardly any term in the realm of information technology seems to be as inappropriately chosen as that of the Demilitarized Zone, which is more often simply referred to by the abbreviation DMZ.

Originally, the term refers to a strip of territory between North and South Korea, in the middle of which runs the demarcation line. Such a zone is usually imagined as an area in which neither attackers nor defenders are present and which is respected by both sides as impassable. This has very little in common with the DMZ, for which this term is used in the field of information technology. This should rather be called a war zone, since here, figuratively speaking, those who have overcome the front line in the form of the firewall are prevented from advancing further by all conceivable means. This should already make it clear where the DMZ is located. Usually, it is located between the internet and the internal networks as an independent network. A DMZ houses servers that should be accessible from the internet. To the extent that a server is accessible from the internet, it must be assumed that it is more at risk from potential attacks than it would be if it were not visible on the internet or could not be reached from there.

Figure 19.1 shows in a very simplified way how, for example, proxy, SFTP or web servers can be positioned in such a network.

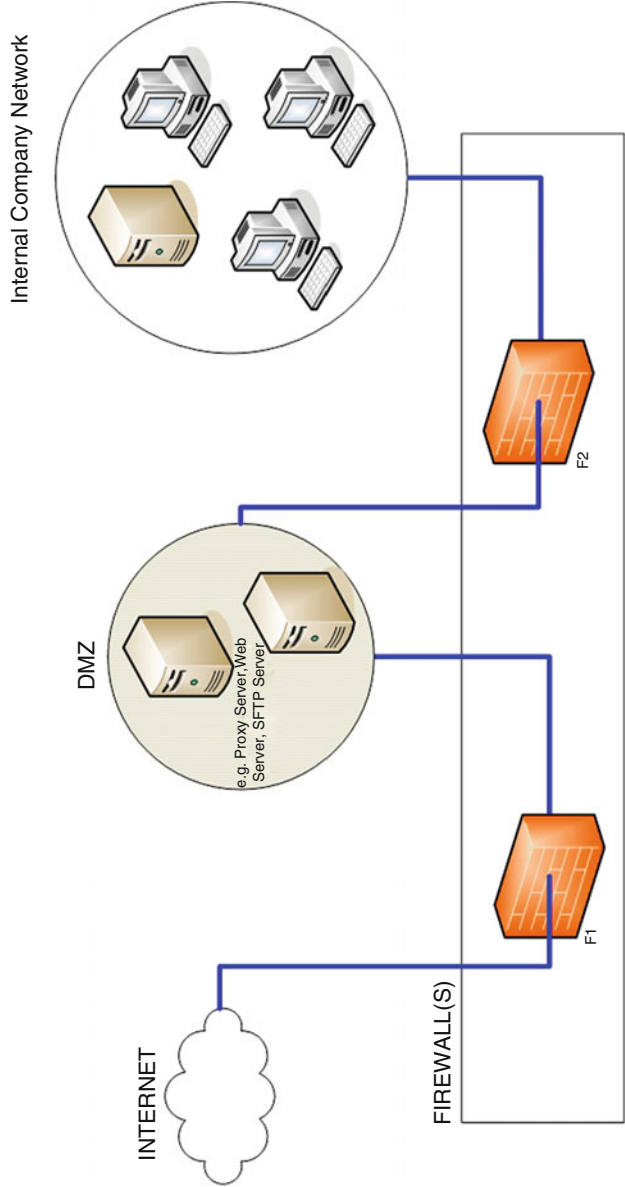


Fig. 19.1 Positioning of a DMZ network

Depending on the size of the company, the number of servers, and the external connections of a company, several DMZ networks can be set up. Differentiation can also be made according to which purposes are to be pursued by the servers in a DMZ area and how strongly individual systems are at risk. Let's assume that a previously unknown security vulnerability is discovered in a base system for web servers. Such vulnerabilities may not be publicly disclosed until a so-called patch, i.e., an update, is already available from the manufacturer to fix the flaw. If a certain web server is now attacked by exploiting this vulnerability before the corresponding update has been made, there is a high probability that the attack will be successful. This would allow a hacker to create a base of operations within a company from which other systems could be attacked if the web server were not quasi-isolated in a DMZ. Communication between the Internet and the webserver requires the server to be accessible from the internet via certain ports. Intelligent firewalls are indeed perfectly capable of detecting various attacks. However, if an attack occurs through the regular channels and is executed due to a security hole in the web server, a firewall would not pose a hurdle. The situation is different if, after a successful attack on the webserver, an injected malware program wants to access the internet as part of further activities or wants to load further malware onto the server. Such requests are often detected by modern firewalls and, if configured correctly, are also prevented.

However, if a hacker has penetrated a server in the DMZ area via a security hole, despite all security precautions, he would still have to overcome another firewall to penetrate the company network or parts of the company network from there, such as separate networks for development or production. Firewalls offer a variety of ways to prevent this. For example, the firewall between the DMZ and the internal network can be configured in such a way that only one or two internal IP or MAC addresses are authorized to access the webserver from the internal network for administrative purposes. The connection request would then always have to originate from the internal authorized device. In this case, a connection request from the DMZ could generally be prevented. Preventing the connection from being established is often referred to as "blocking". The term used inevitably brings us back to military technology. The DMZ is best compared to the kennel of a castle complex. Once the attacker has overcome the first wall, he stands in a deep moat and surely faces another, far higher and more massive wall. He can now neither advance nor retreat and will be massively fought.

Figure 19.1 shows the principle of the DMZ in a very simple way. The blue line shows the connections from the Internet via the firewall into the DMZ network and from the DMZ network via another firewall into the internal company network. In this case, the firewalls F1 and F2 can technically be a single device, which allows

the definition of multiple networks and allows for each network its own rules and filters. The conception and realization of the firewall infrastructure depend on the structure and the protection requirements in the respective company. It is also possible to define additional networks, for example for the accounting department, for the development or patent department, for a company laboratory, or for other sensitive parts of the company IT and to separate them from other networks through a firewall. If a network contains particularly sensitive data and information, all Internet access could also be blocked there, so that it could only communicate with the corporate network in compliance with certain rules and neither connections with the DMZ nor with the Internet would be possible. In practice, there are hardly any technical limits to planning here. Irrespective of the use of a DMZ, the separation of IT areas from parts of the company by firewalls can significantly improve the security level of the company network (see Chap. 17).

However, the DMZ not only offers advantages in terms of a web server that can be reached from the Internet. Proxy servers can also be operated in the DMZ network. These work as a buffer, which means in the example of the web proxy that the request is made from the client computer to the proxy server. The proxy server loads a web page and then makes it available to the requesting client computer. The proxy can fall back on its cache memory so that the construction of a web page that is regularly called via the proxy is usually faster since the request can be answered directly from the proxy's cache memory. Certainly, in times of fiber optic networking and the fast Internet, this functionality no longer plays the role it did a few years ago. However, in places where the "fast" Internet is not yet available, this function will still be appreciated. Another advantage of caching, however, is that the data delivered from the Internet can be comprehensively checked. For example, websites can be checked here for harmful content. As soon as there are concrete indications that visiting or calling up a website could be harmful to a client's computer, the proxy will block access to the site. In addition, a proxy can be equipped with filter functions. Thus, specific web pages can be blocked there that are not necessary for the completion of business tasks or that contain unwanted or illegal information. In such a content filter, for example, pornographic, politically radical or otherwise immoral websites can be blocked. It is also possible to block so-called web mailers, as these are sometimes capable of undermining security precautions concerning a company and can thus pose a threat to a company network. It is also possible to block access to social networks or other portals via such a content filter. In this context, however, it should not go unmentioned that such blocking is not entirely unproblematic, especially if the private use of the Internet as a resource was previously permitted or at least tolerated in the company. The least problematic is therefore blockings that have to be carried out for

comprehensible security reasons and whose omission could pose a threat to systems and data or even to the existence of the company. If content filters are to be used in the company, it is therefore strongly recommended, at least in the European Community, that this be coordinated with the company's data protection officer or an external consultant for data protection issues. In particular, it must be taken into account that such content filters sometimes write log files which make it possible to trace from which computer a certain website was called up. The IP address that is stored in the process is generally to be regarded as personal data so that in the area of application of the European General Data Protection Regulation, such a measure should always be in the focus of data protection.

Just as websites can be checked and filtered, email proxies are also capable of temporarily storing emails and checking emails and attachments for malicious code, even if they are packed. In addition, a SPAM filter can already be used at this point, so that the actual e-mail server is already significantly relieved. From the use of an e-mail proxy at a medium-sized company with around 850 employees, it is known that several thousand spam e-mails are already filtered out on the e-mail proxy every day. If a virus scanner is already in use on the e-mail proxy, it is advisable to use a different virus scanner on the e-mail server. If the end devices are also scanned for viruses, each e-mail would have been scanned three times by different virus scanners before it was read by the recipient. This multi-level approach can significantly reduce the risk of virus contamination of an end device or a corporate network through e-mails (see Chap. 10). The use, type and scope of the corresponding design of a DMZ network should always be planned on a system-specific basis. However, if web servers are not operated externally by a provider but within the company itself, it is generally recommended to separate them in a DMZ.

- **Note 48** *You should always place web servers that are accessible from the Internet and are operated in your own company in a DMZ network or at least outside the central company network.*

At this point, one factor should not be forgotten that often plays an essential role in connection with data security and to which Chap. 9 of this book is dedicated: People! Experience has shown that it is sometimes difficult to prevent the private use of e-mail and the Internet by employees at the workplace. The best argument, however, for establishing proxy servers and content filters in a company is always to consider the dangers posed by private and often at the same time unreflective use, which in the worst case can lead to a production stoppage, company standstill, loss of company secrets and research documents, blatant data protection violations or even the "sudden death" of a company. Viruses and malware do not differentiate

between computers and the activities of employees and managers. This means that the same rules and restrictions should apply to everyone in the company.

- **Note 49** *A computer virus does not distinguish between managers and employees. You should therefore always ensure that company security policies apply equally to all employees.*



Abstract

Technology can significantly increase data security in many ways. However, when secret documents end up in the company's trash, even the best security technology quickly reaches its limits. This shows that data security can only be effectively guaranteed in the company if employees are included in the security considerations just as much as the company's processes and procedures. Therefore, security concepts always require the consideration of organizational measures. This chapter shows an exemplary selection of organizational measures and provides an insight into the wide spectrum beyond technical measures.

Once you, the reader, have reached this chapter, you will understand one thing: That in very few cases is it sufficient for the security of networks to purchase and install only a few technical devices. Just like data protection, data security can only be realized effectively and efficiently if technical equipment and organizational measures are coordinated with each other.

Just as technical measures can be very extensive, the planning and implementation of organizational measures can also reach a high degree of complexity. Therefore, only a small selection of basic organizational measures is listed below in this chapter:

- No unauthorized person may gain physical access to the server or network components. This means that server rooms and network distribution cabinets must be locked and only opened when administrators or authorized persons need to enter the room. A server room must not be open to all personnel as storage (for example, for office supplies) or housing printing stations or paper shredders.

- It must be ensured that no unauthorized person can gain physical access to a workstation computer (for example, when there is no staff in the office).
- Each employee should only have access to the data he or she needs to complete his or her tasks.
- Workstations should only have components that are required. In many cases, for example, a workstation computer doesn't need to be equipped with a DVD drive or a burner. Therefore, you should purchase computers already in the configuration that is required. (Note: This can save company a lot of money).
- Make sure that no private storage devices can be connected to any of your company's computers.
- Pay attention to the safety of the building and its surroundings.
- Make employees aware of data security and data protection.
- Establish binding rules for handling data and IT systems in the company or organization.
- Printouts and paper documents with sensitive content do not belong to household waste.



Abstract

Following the intention of communicating data security in a comprehensible way, the previous chapters of this publication have formulated principles that, if observed, are quite suitable for preventing significant dangers to data security. These principles are summarized again in this chapter and are intended to allow the reader to perform a step-by-step check, similar to a checklist, to determine the extent to which the principles mentioned have already been taken into account in the company or organization. In the end, the reader will have a more or less comprehensive list of what improvements would be useful for data security. Although this list can never replace an audit by an expert, it does provide insights that make it possible to make an initial assessment of the security level in the company or organization.

1. Avoid placing computer or telephone systems, especially server rooms or parts of data centres, in underground cellars or garages. Such systems should be located in the middle of a building (BSI2016-1).
2. Terminal devices such as workstation computers, monitors and printers at the workplace should always be switched off when they are not needed (for example, outside office hours).
3. Avoid the use of cascaded sockets. The electrical supply of IT systems must be carefully planned by a specialist.
4. Never operate a server without protection by a sufficiently dimensioned uninterruptible power supply.

5. Regularly check whether security-relevant updates are available for software or operating systems in use.
6. Do not use an outdated operating system.
7. Never connect a found, unknown or unchecked USB flash drive or other removable media (DVD, ¹ external hard drive) to a productive computer system.
8. If sensitive data is stored on a mobile device, encrypt media or data using the best method available and do not leave the device unattended.
9. Don't let anyone touch your computers with the opinion that you don't need antivirus programs or firewalls.
10. Do not connect critical infrastructure to the internet.
11. As soon as a computer is connected to the internet, it is essential to protect it with professional security software and adequate hardware and to update the systems regularly.
12. Never get into a dispute with your IT administrator. If you are forced to fire him, do not hesitate for a moment and change all relevant passwords and access codes immediately.
13. Prevent any possibility of access to computer systems, network components and central communications equipment, especially firewalls and routers, by unauthorized persons.
14. Never rely solely on the alleged security of an operating system.
15. Use a technical solution to prevent the unauthorized use of mobile data carriers
16. If it is necessary to store sensitive data on an external/mobile device, use only devices with sufficiently strong encryption or store pre-encrypted files on a device.
17. Never integrate telephone components into the computer network where your servers and clients communicate.
18. Never open more communication ports and connection options in a firewall than are absolutely necessary for planned connections.
19. Never connect a critical infrastructure to the internet or to a telephone system that has an internet connection.
20. Protect all components and devices of computer and telecommunication systems against unauthorized access and unauthorized use.
21. When it comes to data security, don't trust that employees will comply with the company's policies.
22. Access rights should be comprehensively documented. No employee may have more access rights than they need to fulfill their operational duties.

¹Digital Versatile Disc.

23. Use only secure methods for data deletion.
24. Don't forget trade secrets or sensitive data on segregated devices.
25. Make sure that not only data but a complete system can be recovered.
26. Test the data backup regularly.
27. Keep encrypted backups safe outside of the office.
28. Only use complex passwords!
29. For all login procedures, the number of possible failed connection attempts should be limited.
30. Never use a factory default password for a system connected to the internet.
31. Never use systems with insecure login procedures, especially when connected to the internet.
32. Always lock your computer's console when you leave the office or workplace.
33. Activate the password protection in the screen saver of your computer if it cannot be ruled out that other persons gain physical access to the system.
34. Note that sometimes the print jobs of several years may be stored on internal hard disks in printer stations or multifunction devices. This is especially important when returning devices to a leasing company.
35. The administrative rights are intended exclusively for administering systems. They should in no case be used for daily work on the PC.
36. Do not use nice-to-have technology. Especially in very complex or critical infrastructures, it is often best to plan and operate communication systems according to conservative approaches. Too much innovation in the area of IT can threaten the existence of a company.
37. Before implementing new technologies, evaluate systems thoroughly and analyze them, especially concerning security issues.
38. A firewall that is suitable for professional purposes can reduce the dangers of new technologies.
39. Firewalls should always be state of the art.
40. Ask an expert to hack into your system to improve data security. But do not give him any passwords for this purpose.
41. Never connect a router to the internet if it does not have a professional firewall or an additional firewall.
42. In larger organizations and companies, it makes sense to also separate network segments (department networks) from each other using firewalls.
43. If resources or know-how for the effective use of security systems are not available within the company, you should have such a system managed by reliable external experts.
44. Do not rely on marketing or advertising claims when selecting security systems.

-
45. The selection of security software that is to be operated without additional purchased services should therefore always be preceded by a comprehensive evaluation.
 46. Comprehensive support should be ensured for self-managed security software. This includes in particular the possibility of contacting support by telephone at short notice.
 47. Where a complex IT infrastructure is in place and where it is possible to do so, different anti-virus and protection systems should be used, complementing each other in multi-stage checks.
 48. You should always place web servers that are accessible from the internet and are operated in your own company in a DMZ network or at least outside the central company network.
 49. A computer virus does not distinguish between managers and employees. You should therefore always ensure that the company security policy applies equally to all employees.

Closing Words

Congratulations! You have reached the end of the extended second edition of this publication, even if it takes a while to read into this exceedingly complex topic. However, please remember that this book is only a brief introduction to the broad field of data security. However, it will still help you to better understand the numerous interactions in a conglomerate of technical parameters that need to be taken into account in order to realize a high level of data security. Especially after the entry into force of the European Data Protection Regulation, data security and the state of the art are receiving significantly more attention than before. However, the threats to data and systems are also constantly evolving.

If reading this book has changed the way you deal with data and systems, then recommend it to your friends, acquaintances and colleagues. Of course, you are also welcome to contact the author if you have questions about data security or data protection. You can reach him via the following website: <https://www.it-planung.com>

Only when we know the dangers of IT use can we act in an appropriate manner. And ultimately, through data security and data protection measures, we protect not only systems and data, but also the freedom of all of us.

Rodalben, July 2021

Literature

- BSI2016-1 (2016) BSI-Grundschrift Maßnahmenkatalog, M 1.13, Bundesamt für Sicherheit in der Informationstechnik (GER)
- Dausch M (2014) Netzwerke-Grundlagen. Herdt-Verlag, Bodenheim
- DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- European Normative 50173-1:2011 about Information technology – generic cabling systems – part 1: general requirements
- Garfinkel S (1996) PGP – pretty good privacy. O'Reilly/International Thomson Verlag, Bonn
- Garfinkel S, Spafford G (1996) Practical unix & internet security, 2nd edn. O'Reilly & Associates Inc., Bonn
- Greguš M, Lenhard TH (2012) Case study – virtualisation of servers in the area of healthcare-IT. (Erschienen in International Journal for Applied Management Science & Global Developments). Biblioscient Publishing Services, Birmingham
- Hunt C (2002) TCP/IP Netzwerk Administration, 3rd edn. O'Reilly Media Inc., Sebastopol (USA)
- Kurtz G, McClure S, Scambray J (2000) Das Anti-Hacker-Buch. MITP-Verlag, Bonn. ISBN 3-8266-4072-1
- Lenhard TH, Kazemi R (2016) Cyberkriminalität und Cyberschutz für Rechtsanwälte und Mandanten. Deutscher Anwaltsverlag, Bonn. ISBN 978-3-8240-5776-4
- Muench P (2010) Technisch-organisatorischer Datenschutz, 4. Aufl. DATAKONTEXT, Heidelberg, S 202. ISBN 978-3-89577-586-4
- Rieger F (2011) Ein amtlicher Trojaner – Anatomie eines digitalen Ungeziefers. Frankfurter Allgemeine Zeitung. <https://www.faz.net/aktuell/feuilleton/ein-amtlicher-trojaner-anatomie-eines-digitalen-ungeziefers-11486473.html>. Accessed 27.07.2021
- Schneier B (1996) Angewandte Kryptographie. Addison-Wesley, Bonn. ISBN 3-89319-854-7

Further Reading

<https://www.britannica.com/technology/protocol-computer-science> . Accessed 10 July 2021
<https://www.dallasnews.com/news/news/2010/11/30/wikileaks-suspect-believed-to-have-used-cd-memory-stick-to-get-past-pentagon-security>. Accessed 27 July 2021
<http://ec.europa.eu/justice/data-protection/>. Accessed 28 Dec 2016
<http://heartbleed.com>. Accessed 12 Jan 2017
<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>. Accessed 27 July 2021
<http://www.netzwerke.com/OSI-Schichten-Modell.htm>. Accessed 31 Mar 2016

Index

A

Access, 9, 28, 29, 32–35, 37–39, 46, 47, 49, 52, 53, 68, 70, 73, 78, 82, 87, 95, 96, 99, 100, 102
Access code
 access rights, 35, 102
Accesses, viii
Address blocks, 13
Administrator privileges, 74–75
Air conditioning, 20
Algorithms, 29, 58, 65, 66, 68, 90
Anti-virus (AV), 32, 34, 42, 90, 91, 104
Antivirus program
 asymmetric, 66, 67
 attachments, 27

B

Backdoor, 39
Background process, 9
Backup, 15, 21, 61–64, 66, 103
Bare metal recovery backup, 62
Binary code, 11
Bomb, logical, 34, 35, 51
Bot virus, 75
Bridge, 37
Brute force attack, 66, 67
Bytes, 10, 11, 13

C

Client, 47, 82, 89, 92, 96, 102
Command shell
 commissioning, 19, 38, 46
Communication port, 47, 102

Communication standard, 2
Company network, 37, 46, 52, 90, 95–97, 104
Computer forensics, 57
Computer Telephony Integration (CTI), vii, 38, 46, 47
Computer virus, 31, 74, 98, 104
Connection control, 8
Content Management System
 controlled shutdown, 23
Copper line
 critical, 6, 23
Cryptography, 2, 65
CTI solution, 37, 47
Current, 22, 23, 49, 64, 91
Cybercrime, 2

D

Damaged, 15, 16, 21, 23, 57, 62
Data, vii, 2–4, 6, 9, 15–16, 19, 20, 22–24, 26, 27, 29–39, 43, 46, 48, 49, 51, 52, 55–64, 66, 67, 70, 73, 78, 82, 87, 88, 96, 97, 100, 102, 103, 105
Data backup, 34, 59, 61–64, 103
Database, 21, 23, 24, 35, 36, 61–63, 70
Database management system (DBMS), vii, 62
Database server, 23
Data carrier, 23, 42, 43, 56–58, 102
Data carrier, memory chip based, 58
Data deletion, 103
Data destruction, 55–60
Data Encryption Standard (DES), vii, 68
Data link layer, 6

- Data loss, 15, 16
- Data packet, 8, 10, 35, 37, 38, 82, 92
- Data protection, 3, 4, 20, 52, 53, 97, 100, 105
- Data security, 2–5, 16, 19, 20, 23, 52, 53, 83, 97, 99–100, 102, 103, 105
- Data spying, 27, 35, 36
- Data theft, 52
- Debug code, 25
- Default password, 69, 70, 103
- Delete, secure, 57
- Demilitarized zone, vii, 93–98
- Detector, 19
- Device, mobile
 - distributors, 36
- DMZ network, 87, 94–97, 104
- Domain controller, 83
- Domain Name Service (DNS), vii, 12

- E**
- Email, 27, 31, 34, 68, 78, 79, 97
- Emergency plan, 20
- Employees
 - encryption, 43
- End-to-end encryption, 68
- Evaluation, 90, 104
- ext3
 - external, 56

- F**
- Fall Foliage, 31
- FAT32, 56
- Fault current, 22, 23
- Federal Trojan, 28, 29
- File, vii, 2, 8, 9, 24, 27, 28, 34, 43, 52, 56–58, 66, 69, 89, 97, 102
- File Transport Protocol (FTP), vii, viii, 9, 10, 66
- Fire, 20, 21, 34, 61, 64, 102
- Fire protection, 4, 20
- Firewall, 28, 31–33, 37–39, 42, 46–48, 66, 75, 76, 81–83, 86–88, 90, 92, 93, 95, 96, 102, 103
- Formatting
 - free, 56
 - FTP service, 9
- Flooding, 19

- G**
- Gateway, 38, 86
- German Social Accident Insurance (DGUV), 22

- H**
- Hacker, 16, 24, 28, 33, 37, 39, 46, 49, 57, 61, 66, 95
- Hard disk
 - hardware, 15, 16, 29, 37, 41, 56–58, 64, 74
- Head-set, 38
- Heart bleed bug, 26
- Hex code, 7
- High frequency technology, 6
- Hub, 37
- Hypertext Transfer Protocol (HTTP), vii, 9, 10, 12, 13
- Hypertext Transfer Protocol Secure (HTTPS), vii, 9, 10, 12, 66

- I**
- ID, 7, 11
- Image backup
 - incremental, 62
- Information and telecommunication (ITC)
 - system, 19, 21
- Infrastructure
 - inside the firewall, 96
 - internal, 95
- International Organization for Standardization (ISO), vii, 7, 79
- Internet, 2, 5, 6, 9, 11, 12, 23, 27–33, 35, 37–39, 45–49, 56, 57, 64, 66–71, 73, 75–79, 81–83, 86–89, 91–93, 95–97, 102–104
- Internet Protocol (IP), vii, viii, 6, 8–13, 30, 38, 47, 77–79, 81, 82, 95, 97
- Inurl
 - IP address, 69

- IP address, dynamic
 - IP4, 10, 11
 - IP6, 13
- IP6
 - IP-based, 13
- IT infrastructure, 55, 91, 92, 104
- K**
- Kernel, 39
- Key, 29, 65, 67
- Keylogger, 35
- L**
- Language package, 8, 34, 66, 70
- Layer, 6, 8, 9, 35, 86
- Layer model, 6
- Leakage, 19
- Leasing, 74, 103
- Level 6, 9
- Lightning
 - Linux, 56, 66
- Logical link control (LLC)
 - login, 8
- M**
- MAC address, 7–13, 67, 78, 79, 82, 95
 - notation, 7
- Mail attachment, 27
- Malware, 16, 27, 29, 31–33, 35, 75, 82, 88, 91, 95, 97
- Manipulation, 16
- Maximum right, 39, 74
- Measures, 2, 5, 16, 20, 30, 33, 38, 39, 42, 48, 53, 63, 70, 97, 99, 105
- Media access control (MAC), vii, 6–8
- Memory segment
 - Microsoft Windows, 56
- Mobile data medium, 43
- Monitoring tool, 31
- Multifunction device, 74, 103
- N**
- Netstat, 30, 31
- Network, 3, 6, 19, 26, 41, 46, 52, 66, 75, 81, 85, 87, 93, 99, 102
- Network adapters, 7
- Network address, 8, 86
- Network card, 7, 37, 49
- Network connector, 36, 37
- Network distributor, 21, 36, 37
- Network ID, 11
- Network segment, 11, 37, 47, 76, 86, 103
- Network traffic, 35
- NTFS
 - number range, 81, 82
- O**
- Offline backup
 - on the web, 64
- Online database, 70
- Online service, 62, 69
- P**
- Package Sniffer, 35, 38, 39
- Password, 8, 29, 34, 35, 37, 39, 45, 64, 66, 67, 69–71, 73, 74, 83, 102, 103
- Password protection
 - personal, 3, 16
 - physic, 103
 - physical access, 74, 103
- Physical layer, 6, 8
- Ping, 12, 13, 77, 78
- Pioneer buyer, 76
- Port
 - port number, 9, 10, 12
- Post Office Protocol (POP), vii, 9
- Power outage, 24
- Power strip, 21
- Power supply, 15, 21, 24
- Power supply unit
 - pre-encrypted, 43
- Pretty Good Privacy (PGP), vii, 67
- Printer Station
 - private USB sticks, 43
- Print job, 74, 103
- Private key, 67
- Production facility, 76
- Program error, 26
- Programming error, 26
- Protection of personal data, 16

- Protocol
 - protocol (IP), 6, 8, 11, 47
- Proxy functionality, 82
- Public address, 85
- Public key, 67

- R**
- Recovery, 15, 57
- Removable media, 28, 41, 42, 102
- Router, 38, 39, 49, 77, 78, 85–86, 102, 103
- Routing functionality, 86
- Routing table, 86

- S**
- Sabotage, 4, 20, 32, 35, 59
- Scheduler, 27
- Screen saver, 73, 74
- Secure File Transport Protocol
 - security hole, 26, 28, 31, 33, 83, 95
- Secure Sockets Layer (SSL), viii, 68
- Security policy, 98, 104
- Security software, 33, 34, 88–92, 102, 104
- Security systems, 87–92, 103
- Security update, 26, 49, 75
- Segments, 11, 13, 56, 86
- Sequence number, 8
- Server, 1, 5, 9, 12, 17–24, 26, 27, 30, 31, 33, 35, 37, 38, 42, 46, 51, 55, 57, 59, 62, 63, 66, 68, 75, 78, 82, 86, 87, 89–93, 95–97, 99, 101
- Server cabinet, 18, 19
- Server directory, 59
- Server room
 - server service, 9
- Service provider, 90
- Services, 9, 10, 21, 23, 24, 29, 30, 33, 46, 52, 76–79, 86, 87, 90, 104
- Simple Mail Transfer Protocol (SMTP), viii, 9, 10
- Smartphone, 6, 41–43, 75
- Sniffer, 35–39, 49
- Socket
 - software, 10–12, 21, 22, 36, 37, 101
- Software, dangerous, 25
- Software system, 26, 27, 30, 32, 35, 52
- Solid State Disc (SSD), viii, 43, 58
- SPX/IPX, 6
- Spy
 - spying, 35
- SQL query, 38
- Standard gateway
 - state of the art, 36
- Stoned virus, 31
- Storage device, network-based, 56–58, 63, 66, 100
- Structured Query Language (SQL), viii, 38, 70, 71
- Subnet mask, 11
- Support, 27, 46, 51, 61, 86, 89–91, 104
- Switch, 36–38
- Synchronization, fault-tolerant, 8
- System administrator, 34, 39, 74
- System update, 26, 33, 86, 89

- T**
- TCP/IP
 - technical and organisational measures, 3, 20, 87
- TCP packet, 8, 35
- Technical solution, 43, 102
- Telecommunication Network Protocol (TNP), viii, 9
- Telephone network, 48
- Telephone system, vii, 19, 37–39, 45–49, 102
- Telnet (TNP), viii, 9, 10
- Threat, 2, 20, 23, 24, 32, 33, 46, 51, 52, 59, 75, 78, 88, 96, 97, 105
- Transmission Control Protocol (TCP), viii, 6, 8, 47
- Transport layer, 8
- Transport Layer Security (TLS), viii, 68
- Trapdoor algorithm
 - trash, 66
- Trojan, 16, 27–31, 35, 43, 73–75
- Trojan Horse, 16, 27–31, 35, 73

- U**
- Unauthorized accesses, 49, 102
- Uninterruptible power supply (UPS), viii, 21, 24, 101
- Universal Serial Bus (USB), viii, 28, 41–43, 51, 52, 58, 102

Update, 26, 30, 33, 86, 89, 90, 95, 102

URL address, 27

URL path

 USB stick, 28, 41–43, 51, 58

 use, 69

V

Virtual, 62

Virtual Private Network (VPN), viii, 66, 86

Virus, 5, 16, 24, 27, 28, 31–33, 41–43, 51,
 61, 64, 74, 75, 82, 86, 88, 91, 97, 98,
 104

Voice over IP, viii, 38

W

Waste water, 19

Water detector, 19

Web browser, 11, 75

Web server

 web-based, 87

Website

 wireless, 67, 68

Wireshark, 35, 36, 38

WLAN router, 78

Working console, 73, 74

World Wide Web, 32